Finanzdirektion  
Amt für Informatik und Organisation

Anhang «Kontrolle und ISDS»

vom [DATUM]

zum (Rahmenvertrag oder Bestellung betreffend …]

1. Vorbemerkungen
   1. Zum Zwecke der Erfüllung des Rahmenvertrages erhält die Leistungserbringerin Zugang zu personenbezogenen Daten, die die Leistungserbringerin durch die Leistungsbezügerin direkt oder in dessen Auftrag durch Dritte offengelegt oder auf andere Weise zur Verfügung gestellt werden (nachfolgend personenbezogene Daten).
   2. Die Parteien stellen sicher, dass die durch die Leistungserbringerin im Auftrag der Leistungsbezügerin direkt oder durch Dritte durchgeführte Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags sowie weiteren Leistungen dem KDSG und dessen Ausführungsbestimmungen entsprechen und die kantonalen Weisungen bezüglich Informationsschutz umgesetzt werden.
2. Geltungsbereich und Gegenstand
   1. Der vorliegende Anhang gilt für jede Form der Verarbeitung personenbezogener Daten für die Leistungsbezügerin durch die Leistungserbringerin.
   2. Gegenstand und Dauer sowie Art und Zweck der Verarbeitung ergeben sich aus dem Rahmenvertrag oder Einzelaufträgen, sofern sie nicht bereits im Rahmenvertrag und in der zugehörigen Leistungsbeschreibung genügend konkretisiert sind.
   3. Die Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen sind in Referenz Dokument spezifiziert, sofern sie nicht bereits im Rahmenvertrag und in der zugehörigen Leistungsbeschreibung genügend konkretisiert sind.
3. Generelle Bestimmungen
   1. Bezüglich den Begriffsdefinition wird auf den Anhang «Glossar» verwiesen.
   2. Aufsicht und Kontrolle
      1. Kontrollrechte

Die Leistungserbringerin räumt folgenden Stellen des Kantons Bern im Rahmen deren gesetzlichen Aufgaben ein Kontrollrecht gemäss den gesetzlichen Grundlagen ein:

1. der Datenschutzaufsichtsstelle des Kantons Bern; sowie
2. der Finanzkontrolle des Kantons Bern.
   * 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 des KAIO oder der mit dem Audit beauftragten Organisation auf eigene Kosten 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 grundsätzlich selber. Die Rechnungen betreffend Audit werden ausschliesslich an das KAIO gestellt. Das KAIO wird die Kosten wie oben beschrieben an die Parteien weiterverrechnen.

Ist die Leistungserbringerin nach anerkannten Informationssicherheits- und Datenschutzstandards zertifiziert, und wird sie in diesem Zusammengang regelmässig auditiert, lässt sie dem Leistungsbezüger den Auditbericht zukommen, soweit dieser Daten, Systeme und Prozesse des Leistungsbezügers betrifft.

* 1. Informationssicherheit und Datenschutz (ISDS)
     1. Grundsätze

Die Leistungserbringerin stellt mit technischen und organisatorischen Massnahmen sicher, dass sie, ihre Angestellten und 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. ISDS-Massnahmen gemäss Konzept vom ……
2. AGB ISDS (V3.0) inkl. Anhang ISDS Grundschutz
3. Weisung des KAIO über den Umgang mit Authentisierungsmerkmalen (IWS 1.3.004)
4. NSP BE Network Security Policy Kanton Bern (IWS 1.3.011)

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 und auf eigene Kosten zu absolvieren.

* + 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. Die Leistungserbringerin betreibt ein Risikomanagement bezüglich der IT-Sicherheit als Teil des auf dem ISO/IEC 2700X 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 Daten betreffen, die mit den Leistungen aus diesem Vertrag im Zusammenhang stehen.

[Wenn noch nicht alle ISDS-Unterlagen bestehen:] Das vom KAIO zu erstellende ISDS-Konzept und die dort beschriebenen Massnahmen sind Teil der Leistungen der Leistungserbringerin. Sie wirkt bei der Erstellung dieser ISDS-Unterlagen auf eigene Kosten mit.

[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.

\* \* \*