Allgemeine Geschäftsbedingungen des Kantons Bern über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen V3.0 (AGB ISDS)

1. Allgemeine Bestimmungen

1.1 Zweck

Diese AGB bezwecken den Schutz der Persönlichkeitsrechte der Personen, deren Daten bearbeitet werden, und die Gewährleistung der Informationssicherheit bei der Erbringung von Informatikdienstleistungen durch Dritte für den Kanton Bern.

1.2 Begriffe

a) *Leistungserbringende:* Natürliche und juristische Personen sowie öffentlich-rechtliche Institutionen, die für den Kanton Bern Informatikdienstleistungen erbringen.

b) *Leistungsbezüger:* Der Kanton Bern, vertreten durch seine Organe oder Dienststellen wie Regierungsrat, Direktionen, Staatskanzlei, Organisationseinheiten, Ämter, Betriebe und Gerichte, die den Leistungserbringer mit der Erbringung von Informatikdienstleistungen beauftragen.

c) *Informatikdienstleistungen:* Leistungen im Bereich der Informatik oder Telekommunikation, insbesondere Kommunikationsdienste, Rechenzentrumsdienste, Aufbau und Betrieb von Büroinformationssystemen, Anwendungsentwicklung und -wartung.

1.3 Gegenstand und Geltung

[1] Diese AGB gelten für die Informatikdienstleistungen, die die Leistungserbringerin oder der Leistungserbringer für die Leistungsbezüger erbringt und die die Bearbeitung von Daten des Leistungsbezügers beinhalten sowie für die damit verbundenen Geschäftsprozesse der Leistungserbringerin oder des Leistungserbringers.

[2] Diese AGB gelten auch für Subunternehmerinnen oder -unternehmer, Beauftragte, Hilfspersonen und Mitarbeitende der Leistungserbringerin oder des Leistungserbringers, die im Zusammenhang mit Daten, Systemen und Prozessen des Leistungsbezügers tätig werden.

1.4 Verhältnis zur vertraglichen Regelung

[1] Die vorliegenden AGB sind Teil eines Vertrags zwischen Leistungserbringerin oder Leistungserbringer und Leistungsbezüger. Sieht dieser vor, dass weitere AGB zur Anwendung kommen, namentlich die „AGB für IKT-Leistungen der Schweizerischen Informatikkonferenz“ (AGB SIK), treten die Bestimmungen der vorliegenden AGB an die Stelle der Informationssicherheits- und Datenschutzbestimmungen der weiteren AGB.

[2] Im Übrigen gehen die Bestimmungen der anderen Vertragsbestandteile den vorliegenden AGB vor.

2. Rechte und Pflichten der Parteien

2.1 Informationspflichten

[1] Die Leistungserbringerin oder der Leistungserbringer informiert und dokumentiert die Leistungsbezüger auf Anfrage über die Methoden und Prozesse, die sie oder er zur Erbringung ihrer/seiner vertraglichen Leistungen einsetzt, und die für die Einhaltung von ISDS relevant sind. Die Leistungsbezüger können die entsprechenden Unterlagen vor Ort einsehen und sich die betrieblichen Abläufe vorführen lassen.

[2] Die Leistungserbringerin oder der Leistungserbringer informiert den Leistungsbezüger unverzüglich über aussergewöhnliche Vorfälle, die die Daten, Systeme und Prozesse des Leistungsbezügers betreffen, namentlich über bedeutende ISDS-Verletzungen.

2.2 Einhaltung des ISDS-Grundschutzes

Die Leistungserbringerin oder der Leistungserbringer stellt den ISDS-Grundschutz gemäss Anhang 1 zu den vorliegenden AGB sicher. Leistungsspezifische Präzisierungen des ISDS-Grundschutzes sind im Vertrag zu regeln.

2.3 Einhaltung zusätzlicher ISDS-Vorgaben gemäss ISDS-Konzept

Übersteigen die ISDS-Ansprüche des Leistungsbezügers das Niveau des ISDS-Grundschutzes, enthält der Vertrag ein ISDS-Konzept, das die entsprechenden Anforderungen und Massnahmen regelt.

2.4 Pflichten gemäss Datenschutzgesetz

Die Leistungserbringerin oder der Leistungserbringer nimmt zur Kenntnis, dass Artikel 16 des kantonalen Datenschutzgesetzes vom 19. Februar 1986 (DSG, BSG 152.04) bestimmt:
„Wer Personendaten im Auftrag einer Behörde bearbeitet, untersteht dem Gesetz wie der Auftraggeber. Zur Bekanntgabe von Personendaten an Dritte bedarf er der ausdrücklichen Zustimmung des Auftraggebers.“[1]

2.5 Beizug von Dritten

[1] Der Vertrag bzw. die weiteren anwendbaren AGB regeln, ob und unter welchen Umständen die Leistungserbringerin oder der Leistungserbringer Dritte beiziehen darf. Die schriftliche Verpflichtung zur Vertraulichkeit gemäss Absatz 2 ist aber auf jeden Fall Voraussetzung für den Beizug Dritter.

[2] Die Leistungserbringerin oder der Leistungserbringer verpflichtet die beigezogenen Dritten (Ziff. 1.3 Abs. 2 der vorliegenden AGB) schriftlich zur Einhaltung der Vertraulichkeit (Ziff. 2.6) und schreibt die Einhaltung der gesetzlichen und vertraglichen ISDS-Bestimmungen im Arbeitsvertrag mit an den Leistungsbezüger verliehenem Personal vor. Sie oder er informiert diese Dritten über die gesetzlichen und vertraglichen ISDS-Bestimmungen.

[1] Die jeweils aktuelle Fassung dieses Gesetzes ist über die Bernische Systematische Gesetzessammlung BSG im Internet verfügbar (www.sta.be.ch/belex).

2.6 Vertraulichkeit

[1] Tatsachen und Daten, die weder offenkundig noch allgemein zugänglich sind, sind geheim zu halten. Im Zweifelsfall sind Tatsachen und Daten vertraulich zu behandeln. Die Geheimhaltungspflichten bestehen schon vor Vertragsabschluss und auch nach Beendigung des Vertragsverhältnisses bzw. nach Erfüllung der vereinbarten Leistung. Vorbehalten bleiben gesetzliche Aufklärungspflichten.

[2] Die Leistungserbringerin oder der Leistungserbringer darf die Tatsache und den wesentlichen Inhalt der Offertanfrage möglichen zu beauftragenden Dritten bekannt geben. Werbung und Publikation über projektspezifische Leistungen bedürfen der schriftlichen Zustimmung des Leistungsbezügers.

2.7 Weitergabe von Daten und Informationen

[1] Die Leistungserbringerin oder der Leistungserbringer darf Daten des Leistungsbezügers ohne anderslautende Ermächtigung nur für diesen verwenden und nur diesem bekannt geben. Begehren um Datenbekanntgabe von Privaten (ob von der Datenbearbeitung betroffen oder nicht), von anderen Behörden oder von anderen Stellen der kantonalen Verwaltung sind an den Leistungsbezüger weiterzuleiten.

[2] Vorbehalten sind gesetzlich vorgesehene prozessuale Zwangsmassnahmen der zuständigen Behörden. Auch in diesen Fällen ist der Leistungsbezüger unverzüglich zu informieren bzw. es ist an ihn zu verweisen, soweit dies gesetzlich zulässig ist.

2.8 ISDS-Audits

[1] Der Leistungsbezüger kann, bezogen auf seine Daten, Systeme und Prozesse, bei der Leistungserbringerin oder dem Leistungserbringer ISDS-Audits durchführen lassen. Die Audits erfolgen nach allgemein anerkannten Methoden durch interne oder externe, fachlich unabhängige und sachkundige Stellen. Die Leistungserbringerin oder der Leistungserbringer ist nicht verpflichtet, mit Auditoren zusammenzuarbeiten, mit denen sie oder er in einem Konkurrenzverhältnis steht. Der Leistungsbezüger lässt der Leistungserbringerin oder dem Leistungserbringer den Auditbericht zukommen.

[2] Ist die Leistungserbringerin oder der Leistungserbringer nach allgemein anerkannten Informationssicherheits- und Datenschutzstandards zertifiziert und wird sie oder er in diesem Zusammenhang regelmässig auditiert, lässt sie oder er dem Leistungsbezüger den Auditbericht zukommen, soweit dieser die Daten, Systeme und Prozesse des Leistungsbezügers betrifft.

[3] Der Vertrag regelt nötigenfalls die Einzelheiten.

2.9 Aufsicht und Kontrolle

[1] Die Leistungserbringerin oder der Leistungserbringer untersteht, soweit Daten, Systeme und Prozesse der Leistungsbezüger betroffen sind, der Aufsicht durch die kantonale Datenschutzaufsichtsstelle (Art. 32ff. DSG), unterstützt durch die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten (IT-SIBE) des kantonalen Amts für Informatik und Organisation.

[2] Die Datenschutzaufsichtsstelle kann im Rahmen ihrer gesetzlichen Aufgaben Kontrollen durchführen oder durchführen lassen. Die Leistungserbringerin oder der Leistungserbringer unterstützt sie dabei unentgeltlich.

2.10 Unterstützung durch den Leistungsbezüger

Der Leistungsbezüger unterstützt die Leistungserbringerin oder den Leistungserbringer bei der Umsetzung ihrer oder seiner Pflichten nach Massgabe der vorliegenden AGB.

3. Sanktionen

Bei der Verletzung der Ziffern 2.5 Abs. 2, 2.6 und 2.7 dieser AGB kommen die Bestimmungen von Ziffer 13.4 AGB SIK Anwendung.

4. Gerichtsstand und anwendbares Recht

Wenn die anderen Vertragsbestandteile den Gerichtsstand oder das anwendbare Recht nicht regeln, ist Gerichtsstand Bern und kommt Schweizer Recht zur Anwendung.

Anhang 1: ISDS-Grundschutz

Die ISDS-Grundschutzmassnahmen sind gestützt auf die Direktionsverordnung vom 3. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV, BSG 152.040.2) für alle Datenbearbeitungen des Kantons umzusetzen.

In der Folge werden diejenigen Bestimmungen des Grundschutzmoduls der ISDS-Wegleitung des kantonalen Amts für Informatik und Organisation wiedergegeben, die im Verantwortungsbereich der Leistungserbringenden liegen. Leistungsspezifische Präzisierungen sind im Vertrag zu regeln (Ziff. 2.2 der AGB ISDS).

1. Zutrittskontrolle (physisch)

Ziel: Verhinderung des Zutritts Unberechtigter zu Räumen, in denen Daten des Leistungsbezügers bearbeitet werden.

1.1 Organisatorische Massnahmen

1.1.1 Sensitive Räumlichkeiten (Bsp. Serverräume, Räume mit wichtigen Telekommunikationseinrichtungen, Räume für Backup-Kopien, Archive) müssen Sicherheitszonen zugewiesen werden.

1.1.2 Der Zutritt zu Informatikräumen und -mitteln ist mittels einer verbindlichen und nachvollziehbaren Zutrittsberechtigung zu regeln. Diese sollte sinnvoll abgestuft sein.

1.1.3 Es ist ein Schliessplan zu erarbeiten und zu dokumentieren, welcher Verantwortlichkeiten, Verwaltung, Vergabe und Rücknahme der Zutrittsmittel regelt.

1.2 Technische Massnahmen

1.2.1 Die Eingänge zu den Sicherheitszonen müssen über ein sicheres Schliess- und Zutrittssystem verfügen.

1.2.2 Schliess- und Zutrittssysteme müssen regelmässig auf ihre korrekte Funktionsweise überprüft werden.

1.2.3 Der Zutritt durch andere Gebäudeöffnungen ist durch raumsichernde Massnahmen, wie Fenstervergitterungen, Sicherheitsstoren usw. zu verhindern.

2. Zugangskontrolle

Ziel: Verhinderung der Nutzung von IT-Anlagen, -Diensten, -anwendungen und Kommunikationseinrichtungen und Einsicht in Datenausgaben des Leistungsbezügers durch Unbefugte.

2.1 Organisatorische Massnahmen

2.1.1 Die Vergabe von Benutzerrechten muss verbindlich geregelt, dokumentiert und überwacht werden.

2.1.2 Accounts und Zugriffsrechte, die die nicht mehr benötigt werden (z.B. wegen Austritts) oder die über längere Zeit nicht mehr benutzt worden sind, müssen gesperrt oder gelöscht werden.

2.1.3 In publikumszugänglichen Bereichen (z.B. Schalter, Sekretariaten) sind periphere Geräte wie Bildschirme und Drucker so zu platzieren, dass Unberechtigte keinen Einblick in die Daten haben.

2.2 Technische Massnahmen

2.2.1 Die Zugangsberechtigung auf Systeme erfolgt mit einer Benutzeridentifikation und einem sicheren Passwort. Für Passworte gilt:

- Passworte sind persönlich und geheim.
- Sie umfassen mindestens 8 Stellen und sind unter Verwendung von Buchstaben und Sonderzeichen oder Zahlen zu bilden.
- Das Passwort darf nicht identisch mit dem Benutzernamen sein.
- Die Gültigkeit ist beschränkt auf höchstens 30 Tage oder auf max. 3 Fehlversuche.

2.2.2 Nach max. 3 Fehlversuchen muss die Zugangsberechtigung gesperrt werden.

2.2.3 Fehlgeschlagene Zugriffsversuche (Sperren von Accounts) müssen protokolliert und die Protokolle regelmässig ausgewertet werden.

3. Zugriffskontrolle (logisch)
Ziel: Verhinderung von unbefugten Zugriffen auf Daten des Leistungsbezügers durch berechtigte Systembenutzende.

3.1 Organisatorische Massnahmen:

3.1.1 Erarbeiten und Einrichten eines zweckmässigen und verbindlichen Berechtigungskonzepts auf der Basis definierter Benutzerrollen.

3.2 Technische Massnahmen:

3.2.1 Benutzer müssen sich mit einer persönlichen User-ID und einem sicheren Passwort gegenüber dem System identifizieren und authentifizieren (siehe oben Ziffer 2).

4. Weitergabekontrolle
Ziel: Verhinderung des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität der Daten des Leistungsbezügers während der Übermittlung.

4.1 Organisatorische Massnahmen

4.1.1 Es sind Weisungen für die Verwendung von Datenübertragungsmitteln (Fax, Internet, Handy usw.) zu erlassen.

4.1.2 Datenträger (Papier, Disketten, CDs, usw.) mit klassifizierten Daten müssen als solche bezeichnet und erkennbar sein.

4.1.3 Datenträger sind für den Versand geeignet zu verpacken und zu adressieren.

4.1.4 Es muss festgelegt und kontrolliert werden, welche Benutzer und Betreiber welche Netzwerkdienste beanspruchen dürfen.

4.2 Technische Massnahmen

4.2.1 Die Vertraulichkeit und Integrität von Authentifikationsdaten, Schlüsseln oder anderen kritischen Systemdaten muss bei der Übertragung der Daten über Netzwerke geschützt werden.

4.2.2 Übertragungen von/zu Fremdnetzen müssen protokolliert werden (Verbindungsaufbau, Benutzer).

5. Eingabekontrolle
Ziel: Beweissicherung in Bezug auf die Benutzeraktivitäten.

5.1 Organisatorische Massnahmen:

5.1 Es muss verbindlich geregelt werden, wer welche Daten bearbeiten darf und wer die Verantwortung für den Datenschutz und die Datenqualität trägt.

5.2 Technische Massnahmen:

Keine vorgeschrieben.

6. Auftragskontrolle
Ziel: Gewährleistung der auftragskonformen Bearbeitung der Daten des Leistungsbezügers.

6.1 Organisatorische Massnahmen

(Im Rahmen dieser AGB nicht relevant)

6.2 Technische Massnahmen

6.2.1 Der Zugriff ist auf genau festgelegte Daten und Anwendungen zu beschränken.

6.2.2 Zugriffe über das Netz von aussen sind durch starke Authentifikationsverfahren zu schützen.

7. Verfügbarkeitskontrolle
Ziel: Schutz der Daten des Leistungsbezügers vor eingeschränkter Verfügbarkeit, gegen Zer-

störung und Verlust.

7.1 Organisatorische Massnahmen

7.1.1 Authentifikationsdaten des Systemverantwortlichen oder anderer privilegierter Systembetreiber müssen für notfallmässige Stellvertretungen in sicherer Form hinterlegt sein.

7.1.2 Für die Sicherheit von Betrieb, Nutzung und Wartung von Systemen und Anwendungen notwendige Dokumentationen müssen zu jeder Zeit bei den System- und Anwendungsverantwortlichen verfügbar sein.

7.2 Technische Massnahmen

7.2.1 Informatikräume und -systeme sind gegen physische Einflüsse (Einbruch, Brand, Wasser, usw.) angemessen zu schützen.

7.2.2 Systeme müssen durch einen Überspannungsschutz, eine unterbrechungsfreie Stromversorgung (USV) sowie durch eine entsprechende Klimatisierung geschützt sein.

7.2.3 Das Sichern von Daten auf Datenträgern (Backup) und das Zurückladen der Daten (Restore) muss regelmässig geprüft werden.

7.2.4 Mobile Datenträger müssen an geschützten und räumlich von der Betriebsumgebung abgegrenzten Orten aufbewahrt werden.

8. Trennungskontrolle

Ziel: Sicherstellung der Einhaltung des Zweckbindungsgebotes (Art. 5 Abs. 4 DSG).

8.1 Organisatorische Massnahmen

(Im Rahmen dieser AGB nicht relevant)

8.2 Technische Massnahmen

8.2.2 Test- und Produktionsdaten sind getrennt zu bearbeiten. Eine zuverlässige logische Trennung reicht aus.

(Weitere Bestimmungen im Rahmen dieser AGB nicht relevant)

9. Weitere Kontrollziele

Ziel: Generelle Gewährleistung der Informationssicherheit.

9.1 Organisatorische Massnahmen

9.1.3 Es sind angemessene Vorkehrungen für Stör-, Not- und Katastrophenfälle zu treffen.

(Weitere Bestimmungen im Rahmen dieser AGB nicht relevant)

9.2 Technische Massnahmen

9.2.1 Systeme und Anwendungen sind durch anerkannte Verfahren und Produkte gegen schadenstiftende Software (Viren, Spyware etc.) zu schützen.

(Weitere Bestimmungen im Rahmen dieser AGB sind nicht relevant)

* * *