Allgemeine Geschäftsbedingungen des Kantons Bern

über die

Informationssicherheit und den Datenschutz

AGB ISDS BE

vom 26.08.2024
revidiert 16.12.2024

Version 2.0

Inhaltsverzeichnis

1. Zweck

1.1 Diese Allgemeinen Geschäftsbedingungen über die Informationssicherheit und den Datenschutz (AGB ISDS) bezwecken die Gewährleistung der Informations- und Datensicherheit und damit auch des Datenschutzes bei der Beschaffung und beim Einsatz von ICT-Mitteln durch die Behörden des Kantons Bern.

1.2 Mit der Umsetzung der AGB ISDS sowie der Anforderungen gemäss der Weisung des Amtes für Informatik und Organisation (KAIO) über den Grundschutz für die Informations- und Cybersicherheit (ICSGW)[1] vom 16. Dezember 2024 wird der Grundschutz für die ICT-Mittel, Informationen und Personendaten auch durch die Leistungserbringerinnen sichergestellt.

2. Begriffe

In diesen AGB bedeuten:

2.1 **Behörden:** Auftraggebende kantonale Behörden, die Gemeindebehörden sowie die Träger öffentlicher Aufgaben des Kantons und der Gemeinden unabhängig von ihrer Rechtsform (Art. 4 Abs. 1 und 2 des Gesetzes vom 7. März 2022 über die digitale Verwaltung (DVG)[2]).

2.2 **Leistungserbringerin**: Eine natürliche oder juristische Person, welche im Auftrag einer Behörde diese mit ICT-Mitteln versorgt.

2.3 **ICT-Mittel:** Güter und Dienstleistungen der Informations- und Telekommunikationstechnik (ICT), einschliesslich Hardware und Software (Art. 4 Abs. 3 Bst. a DVG).

2.4 **Informationen:** Angaben in beliebiger Form über Sachverhalte, jedoch ohne Personendaten (Art. 4 Bst. b ICSGW).

2.5 **Personendaten:** Angaben in beliebiger Form über bestimmte oder bestimmbare natürliche oder juristische Personen (Art. 2 Abs. 1 des Datenschutzgesetzes vom 19. Februar 1986, KDSG[3]).

2.6 **Informations- bzw. Datensicherheit:** Zustand, wo die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der ICT-Mittel und Informationen bzw. der Personendaten gewährleistet sind (Art. 4 Bst. d ICSGW).

2.7 **Bearbeiten:** Jeden Umgang mit Informationen oder Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten (Art. 2 Abs. 4 KDSG).

2.8 **Bekanntgeben:** Jedes Zugänglichmachen von Informationen oder Personendaten, wie das Einsichtgewähren, Auskunftgeben, Weitergeben oder Veröffentlichen (Art. 2 Abs. 5 KDSG).

2.9 **Sicherheitsvorfall:** Ein Ereignis, welches die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der ICT-Mittel, Informationen oder Personendaten gefährdet (Art. 4 Bst. f ICSGW) .

[1] ICSGW, Internetseite Datenschutz, Informations- und Cybersicherheit des KAIO
[2] DVG; BSG 109.1
[3] KDSG; BSG 152.04

3. Unterstellung unter das Datenschutzgesetz des Kantons Bern

3.1 Die Leistungserbringerin nimmt zur Kenntnis, dass sie als Auftragsdatenbearbeiterin gemäss Artikel 16 KDSG diesem Gesetz im gleichen Masse wie die auftraggebende Behörde untersteht. Insbesondere bedarf die Bekanntgabe der Personendaten an Dritte der ausdrücklichen Zustimmung der Behörde.

4. Verhältnis zum Vertrag sowie zu den AGB SIK

4.1 Die AGB ISDS sind Teil des Vertrages zwischen der Leistungserbringerin und der Behörde. Vorbehalten bleiben abweichende Vereinbarungen.

4.2 Die Allgemeinen Geschäftsbedingungen für IKT-Leistungen der Schweizerischen Informatikkonferenz (AGB DVS)[4], zum Stand gemäss Vertragsschluss, sind ebenso Teil des Vertrages, gehen aber diesem sowie den AGB ISDS nach.

5. Informations- und Datensicherheit

5.1 Verantwortung

5.1.1 Die Behörde behält die Verfügungsmacht an den in ihrem Auftrag bearbeiteten Informationen und Personendaten; dies gilt sowohl für Inhaltsdaten als auch für Randdaten nach Artikel 1 Absatz 1 Buchstabe a und b der Randdatenverordnung vom 20. November 2019 (RDV)[5]. Sie bleibt für deren Schutz verantwortlich und weisungsberechtigt (Gewährleistungsverantwortung, Art. 8 Abs. 1 KDSG).

5.1.2 Die Leistungserbringerin hat im Rahmen ihres Herrschaftsbereichs für die Sicherheit der ihr anvertrauten ICT-Mittel, Informationen und Personendaten zu sorgen.

5.1.3 Die Leistungserbringerin erwirbt an den bearbeiteten Informationen und Personendaten keine Rechte. Sie hat die ISDS-Massnahmen wirksam umzusetzen und die Weisungen der Behörde zu befolgen (Umsetzungsverantwortung).

5.2 Umsetzung des Grundschutzes

5.2.1 Die Leistungserbringerin hat die Grundschutzmassnahmen gemäss der ICSGW, zum Stand des Vertragsschlusses, umzusetzen und nachweisbar auf ihre Wirksamkeit zu prüfen. Leistungsspezifische Präzisierungen sind im Vertrag geregelt.

5.3 Umsetzung des erhöhten Schutzes gemäss ISDS-Analyse und -Konzept

5.3.1 Führt die ISDS-Analyse der Behörde zum Ergebnis, dass für die zu bearbeitenden Informationen und Personendaten ein erhöhter Schutzbedarf besteht, so sind die dazu erforderlichen und vertraglich, gemäss ISDS-Konzept vereinbarten Massnahmen von der Leitungserbringerin umzusetzen und nachweisbar auf ihre Wirksamkeit zu prüfen (Art. 5 ISDS DV[6]: ISDS-Analyse und -Konzept).

[4] AGB DVS
[5] RDV; BSG 153.011.5
[6] ISDS DV, BSG 152.040.2

6. Datenbearbeitung

6.1 Zweckbindung

6.1.1 Die Informationen und Personendaten dürfen nur durch diejenigen Mitarbeitenden der Leistungserbringerin bearbeitet werden, welche die Informationen und Personendaten zur Erfüllung des Vertrages benötigen. Die Bearbeitung der Informationen und Personendaten darf ausschliesslich zum vertraglich festgelegten Zweck erfolgen.

6.2 Bearbeiten und Bekanntgabe von Informationen oder Personendaten

6.2.1 Die Leistungserbringerin darf Informationen oder Personendaten der Behörde ohne anderslautende Ermächtigung nur für die Behörde bearbeiten oder bekanntgeben. Begehren von Privaten oder anderen Behörden um Datenbekanntgabe sind unverzüglich der Behörde weiterzuleiten.

6.2.2 Vorbehalten sind gesetzlich vorgesehene prozessuale Zwangsmassnahmen anderer zuständiger Behörden. Auch in diesen Fällen ist, soweit gesetzlich zulässig, an die Behörde zu verweisen, oder diese ist unverzüglich zu informieren.

6.3 Ort der Bearbeitung von Informationen und Personendaten

6.3.1 Soweit der Vertrag nichts anderes vorsieht, darf die Bearbeitung der Informationen und Personendaten nur in der Schweiz oder in einem Staat mit einem angemessenen Datenschutz gemäss Anhang 1 der Verordnung des Bundesrates vom 31. August 2022 über den Datenschutz (DSV)[7] erfolgen.

7. Beizug von Subunternehmen

7.1 Der Vertrag regelt, ob und unter welchen Umständen die Leistungserbringerin Subunternehmen beiziehen darf, welche bei direkter Ausübung der ihnen von der Leistungserbringerin übertragenen wesentlichen Leistungen selbst in den Anwendungsbereich der AGB ISDS fallen würden. Soweit bei Vertragsschluss bekannt, werden diese Subunternehmen im Vertrag aufgeführt und deren Einsatz von der Behörde genehmigt.

7.2 Die Leistungserbringerin verpflichtet die Subunternehmen gemäss Ziff. 7.1 vertraglich, die Sicherheitsmassnahmen gemäss Hauptvertrag, ISDS-Konzept sowie gemäss den AGB ISDS als auch AGB SIK umzusetzen.

8. Audits

8.1 Rechtmässigkeitsprüfung

8.1.1 Die Leistungserbringerin räumt folgenden unabhängigen staatlichen Aufsichtsstellen im Rahmen deren gesetzlichen Aufgaben zur Überprüfung der rechtmässigen Leistungserbringung ein Audit- und Kontrollrecht ein:

a) der zuständigen Datenschutzaufsichtsstelle;
b) dem zuständigen Finanzaufsichtsorgan.

[7] DSV; SR 235.11

Die Leistungserbringerin ist im Rahmen der gesetzlichen Grundlagen der Aufsichtsstellen zur Mitwirkung und insbesondere zur Herausgabe der erforderlichen Informationen und Unterlagen verpflichtet.

8.2 Leistungsüberprüfung

8.2.1 Die Behörde kann im Zusammenhang mit den vertraglich vereinbarten Leistungen Audits im Bereich der Informationssicherheit, des Datenschutzes, der Prozesse und der Rechnungsstellung durchführen.

8.3 Durchführung der Audits

8.3.1 Der Behörde obliegt die Leitung des Audits. Sie bestimmt nach Anhörung der Leistungserbringerin

a) die Auditobjekte, wie z.B. Prozesse, Core Services, Software, Datensammlungen, Dokumentationen und Quellcode, Leistungsabrechnungen;
b) die mit dem Audit beauftragte Organisation, wobei es sich nicht um einen direkten Konkurrenten der Leistungserbringerin handeln darf, und
c) das Verfahren und die Einzelheiten des Audits.

8.3.2 Die Behörde wird die Ausübung der Auditrechte grundsätzlich mindestens einen Monat im Voraus ankündigen, unter Darlegung des Auditthemas und –zeitplans. Bei Sicherheitsvorfällen kann die Frist verkürzt werden.

8.3.3 Die Leistungserbringerin wirkt beim Audit gemäss den Weisungen der Behörde 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.

8.3.4 Die Behörde verpflichtet die mit dem Audit beauftragte Organisation und ihre Mitarbeitenden oder Beauftragten zur Verschwiegenheit.

8.4 Kosten

8.4.1 Die Kosten für ein Audit infolge eines hierzu beauftragten Dritten werden grundsätzlich von der Behörde übernommen. Im Übrigen tragen die Parteien die ihnen infolge des Audits angefallenen Kosten grundsätzlich selbst.

8.4.2 Stellt sich anlässlich des Audits heraus, dass gesetzliche oder vertragliche Vorschriften verletzt wurden und von der auditierenden Behörde Feststellungen mittlerer oder hoher Bedeutung gemacht wurden, so gilt jedoch, dass die Leistungserbringerin

a) die infolge nicht gehöriger Vertragserfüllung und der demzufolge zu viel bezogenen Vergütungen, zuzüglich Zins zu 5 %, und
b) alle internen und externen Kosten, die der Behörde im Zusammenhang mit dem Audit entstanden sind,

innert 30 Tagen nach Vorliegen des von der auditierenden Behörde genehmigten Schlussberichts dem Kanton schuldet.

8.4.3 Die Kosten zur Behebung der im Audit festgestellten Mängel gehen zu Lasten der Leistungserbringerin.

9. Meldepflicht und Sofortmassnahmen bei Sicherheitsvorfällen und Schwachstellen

9.1 Die Leistungserbringerin hat die Behörde über Sicherheitsvorfälle oder Schwachstellen gemäss Art. 4 Bst. f und g ICSGW zu informieren und mit der Behörde zusammenzuarbeiten, insbesondere wenn

a) ein Sicherheitsvorfall oder eine Schwachstelle gemäss ICSGW, Anhang 2, Ziff. 1.1.4, vorliegt, oder
b) eine andere ausserkantonale oder ausländische Behörde bei der Leistungserbringerin Kontrollhandlungen und Massnahmen durchführt, soweit sie Informationen, Personendaten oder ICT-Mittel gemäss Vertrag betreffen, oder
c) ICT-Mittel bei der Leistungserbringerin durch Pfändung, Konkurs oder andere Zwangsvollstreckungsmassnahmen oder durch sonstige Ereignisse oder Massnahmen Dritter entzogen werden. Die Leistungserbringerin wird alle hierfür Verantwortlichen unverzüglich darüber informieren, dass die Verfügungsmacht über die Informationen und Personendaten gemäss Vertrag allein bei der Behörde liegt.

Die vorgenannten Sicherheitsvorfälle müssen spätestens innert 24 Stunden, Schwachstellen innert 48 Stunden seit Entdeckung der von der Behörde bezeichneten Stelle gemeldet werden. Der Inhalt der Meldung hat den Anforderungen gemäss der Cybersicherheitsverordnung des Bundes zu genügen.

9.2 Die Leistungserbringerin wird in den vorgenannten Fällen umgehend diejenigen Sofortmassnahmen ergreifen, die rechtlich und nach dem aktuellen Stand der Technik erforderlich sind, um die Informationen und Personendaten und die für deren Bearbeitung eingesetzten ICT-Mittel zu sichern und nachteilige Folgen bestmöglich zu verhindern bzw. zu minimieren.

9.3 Die Leistungserbringerin dokumentiert zu Handen der Behörde die Vorfälle und allfällige Verletzungen der Informations- und Datensicherheit. Zudem ergreift und dokumentiert sie diejenigen Massnahmen, welche nach dem aktuellen Stand der Technik erforderlich sind, um eine Wiederholung der Verletzung zu verhindern.

10. Vertraulichkeit und Personaleinsatz

10.1 Es gelten die Ziff. 13 und 14 der AGB SIK vom Januar 2020, insbesondere auch die dort beschriebenen straf- und privatrechtlichen Sanktionen.

11. Rückgabe und Löschung bei Vertragsende

11.1 Mit Beendigung des Vertrages hat die Leistungserbringerin sämtliche in ihrem Herrschaftsbereich liegenden Informationen und Personendaten im vereinbarten oder einem weiterverarbeitbaren Format gemäss aktuellem Stand der Technik der Behörde unentgeltlich auszuhändigen.

11.2 Durch die Leistungserbringerin bearbeitete Informationen oder Personendaten hat sie gemäss Weisung der Behörde unentgeltlich und gemäss Anforderungen des Anhangs 2 zur ICSWG, Ziff. 1.2.3, nicht wiederherstellbar zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf erste Aufforderung der Behörde vorzulegen.

* * *