Direktionsverordnung über Informationssicherheit und Datenschutz (ISDS DV)

vom 03.01.2011 (Stand 01.04.2011)

Die Finanzdirektion des Kantons Bern,

gestützt auf Artikel 38 des Datenschutzgesetzes vom 19. Februar 1986 (KDSG[1)]) und Artikel 9 der Datenschutzverordnung vom 22. Oktober 2008 (DSV[2)])

beschliesst:

1 Allgemeine Bestimmungen

Art. 1 *Gegenstand*

[1] Diese Verordnung regelt die Grundsätze und das Verfahren zur Umsetzung von Informationssicherheit und Datenschutz (ISDS) beim Einsatz von Informations- und Telekommunikationstechnologie (ICT) durch die Kantonsverwaltung.

Art. 2 *Geltungsbereich*

[1] Diese Verordnung gilt für Projekte, Anwendungen und Komponenten der ICT.

[2] Sie gilt für die ganze Kantonsverwaltung.

[3] Bei der Gewährung von Abgeltungen im Sinne des Staatsbeitragsgesetzes vom 16. September 1992 (StBG [3)]) für ICT-Projekte, deren Datenbearbeitungen dem KDSG unterstehen, haben die Gesuchstellerinnen und Gesuchsteller entweder die materiellen Bestimmungen dieser Verordnung (Art. 5 und die fachlichen Weisungen gemäss Art. 12) oder die Bestimmungen eines ausgewiesenen, anerkannten und gleichwertigen ISDS-Standards einzuhalten.

Art. 3 *Verantwortlichkeiten*

[1] Verantwortlich für ISDS sind diejenigen Stellen, die Daten, insbesondere Personendaten, zur Erfüllung ihrer gesetzlichen Aufgaben bearbeiten oder durch Dritte bearbeiten lassen (verantwortliche Stellen).

[1)] BSG 152.04
[2)] BSG 152.040.1
[3)] BSG 641.1

* Änderungstabellen am Schluss des Erlasses

[2] Bearbeiten mehrere Stellen Daten gemeinsam, so ist schriftlich festzulegen, welche Stelle für ISDS die Hauptverantwortung trägt.

Art. 4 *Pflichten der verantwortlichen Stelle*

[1] Die verantwortliche Stelle sorgt dafür, dass bei allen ICT-Anwendungen, mit denen Personendaten bearbeitet werden, die gesetzlichen und vertraglichen Datenschutzvorschriften eingehalten werden und dass bei der Bearbeitung von Daten die Informationssicherheit in angemessener Weise gewährleistet ist.

2 ISDS bei der Abwicklung von ICT-Projekten

Art. 5 *ISDS-Analyse und ISDS-Konzept*

[1] Bei jedem ICT-Projekt bestimmt der Projektausschuss im Rahmen der Projektorganisation eine ISDS-Verantwortliche oder einen ISDS-Verantwortlichen.

[2] Die verantwortliche Stelle beurteilt in der Phase Voranalyse mit einer ISDS-Analyse die datenschutzrechtliche Konformität des Vorhabens und bestimmt mit einer Schutzbedarfsklassifizierung, ob bei dem Projekt erhöhte ISDS-Anforderungen bestehen.

[3] Erhöhte ISDS-Anforderungen bestehen insbesondere, wenn

a der Wiederbeschaffungswert der Infrastruktur hoch ist,
b ein Ausfall der ICT-Systeme von mehr als einem Arbeitstag gravierende Folgen für die Auftragserfüllung hat,
c eine Wiederherstellung der Daten mit erheblichen Problemen oder Kosten verbunden ist,
d die bearbeiteten Daten besonderen gesetzlichen oder vertraglichen Geheimhaltungsvorschriften unterliegen (z.B. dem Berufsgeheimnis) oder
e eine Datenschutzverletzung für die Betroffenen spürbar nachteilige Folgen hat, was in der Regel bei der Bearbeitung von besonders schützenswerten Personendaten der Fall ist.

[4] Ergibt die ISDS-Analyse, dass keine erhöhten ISDS-Anforderungen bestehen, sorgt die verantwortliche Stelle dafür, dass auf den Zeitpunkt der Inbetriebnahme der ICT-Anwendung die massgeblichen Datenschutzvorgaben eingehalten werden und die Informationssicherheit mindestens durch die Umsetzung der ISDS-Grundschutzmassnahmen gewährleistet ist.

[5] Ergibt die ISDS-Analyse, dass erhöhte ISDS-Anforderungen bestehen, ist spätestens in der Phase Konzept ein ISDS-Konzept zu erstellen. Im Rahmen dieses Konzepts sind auf der Grundlage einer Risikoanalyse

a die nach Umsetzung der ISDS-Grundschutzmassnahmen für eine angemessene Informationssicherheit und einen angemessenen Datenschutz zusätzlich erforderlichen organisatorischen und technischen Massnahmen zu bestimmen sowie

b die Voraussetzungen dafür zu schaffen, dass diese auf den Zeitpunkt der Inbetriebnahme der ICT-Anwendung umgesetzt werden.

Art. 6 *Unterlagen für die Bewilligung von ICT-Projekten und der entsprechenden Ausgaben*

[1] Anträge auf Kreditbewilligungen und Unterlagen zur Vorabkontrolle von Datenbearbeitungen (Art. 17a KDSG) enthalten die erarbeiteten ISDS-Unterlagen. Diese sind von der oder dem ISDS-Verantwortlichen des Projekts zu visieren.

[2] Bestehen bei einem Vorhaben erhöhte ISDS-Anforderungen, enthält der Antrag auf Kreditbewilligung eine Stellungnahme der kantonalen Datenschutzaufsichtsstelle, die beurteilt, ob das KDSG und die anderen ISDS-Bestimmungen eingehalten werden (Vorabkontrollbericht).

[3] ISDS-Unterlagen, die der kantonalen Datenschutzaufsichtsstelle zur Stellungnahme unterbreitet werden, sind gleichzeitig auch dem Informationssicherheitsbeauftragten des Kantons (IT-SIBE) (Art. 10) zuzustellen.

[4] Bei der Gewährung von Abgeltungen an mit ISDS-Auflagen versehene Projekte, für die ein anderer ISDS-Standard gewählt wurde (Art. 2 Abs. 3), treten die nach Massgabe des gewählten ISDS-Standards erforderlichen Dokumente an die Stelle von ISDS-Analyse und -Konzept. In diesem Fall finden Absatz 2 und 3 unabhängig davon Anwendung, ob bei dem Vorhaben erhöhte ISDS-Anforderungen bestehen oder nicht, und auf Anfrage hin sind auch die Unterlagen, die den gewählten ISDS-Standard selbst definieren, zuzustellen.

Art. 7 *Konsequenzen bei Nichteinhalten*

[1] Fehlen die ISDS-Analyse bzw. ein aktuelles ISDS-Konzept oder ergibt sich aus den Abklärungen, dass das Projekt nicht datenschutzkonform oder die Informationssicherheit nicht gewährleistet ist, so erteilt der Auftraggeber die Freigabe der weiterführenden Projektierungsphase nur unter der Bedingung der Behebung der Mängel, und der Betrieb darf nicht vor der Mängelbehebung aufgenommen werden.

[2] Die Informationssicherheit ist insbesondere dann nicht gewährleistet, wenn bei der Inbetriebnahme der ICT-Anwendung noch als hoch bewertete Sicherheitsrisiken bestehen.

3 ISDS bei bestehenden ICT-Anwendungen

Art. 8

[1] Für die ICT-Anwendungen, die nicht bereits im Projektstadium Gegenstand einer ISDS-Analyse waren, ist eine solche zu erstellen.

[2] Für die Anwendungen, bei denen sich auf Grund der Schutzbedarfsklassifizierung ein erhöhter Schutzbedarf ergibt, ist ein ISDS-Konzept zu erstellen, das namentlich eine Risikoanalyse und eine verbindliche Massnahmenplanung zur Beseitigung hoher Risiken umfasst.

4 ISDS bei ICT-Komponenten

Art. 9

[1] ICT-Komponenten sind die körperlichen oder unkörperlichen Teile der ICT-Infrastruktur, die zur elektronischen Datenbearbeitung durch Anwendungen dienen, beispielsweise Geräte mit oder ohne eigene Bearbeitungsfunktionen, Prozesse oder Dienstleistungsangebote («services»).

[2] Für ICT-Komponenten, deren Informationssicherheit und Datenschutz nicht bereits Gegenstand des ISDS-Konzepts eines Projekts oder einer Anwendung sind, ist mindestens der ISDS-Grundschutz sicherzustellen.

[3] Ergibt sich aus ISDS-Anforderungen an Projekte oder Anwendungen, für welche die ICT-Komponenten eingesetzt werden, ein weitergehender Schutzbedarf, nimmt die für das Projekt verantwortliche Stelle die entsprechenden Sicherheits- und Schutzmassnahmen vor oder sorgt für deren Vornahme durch die für die ICT-Komponenten verantwortliche Stelle.

[4] Die Umsetzung der Sicherheits- und Schutzmassnahmen wird in geeigneter Form protokolliert. Der kantonalen Datenschutzaufsichtsstelle und der oder dem IT-SIBE ist auf Anfrage Einsicht in die Dokumentation zu gewähren.

5 Aufsicht und Ausführungsbestimmungen

Art. 10 *Aufsicht*

[1] Die Aufsicht über die Einhaltung der Datenschutzvorgaben und die Gewährleistung der Informationssicherheit obliegt für die Bearbeitung von Personendaten der kantonalen Datenschutzaufsichtsstelle (Art. 34 KDSG).

[2] Die kantonale Datenschutzaufsichtsstelle arbeitet mit der oder dem IT-SIBE zusammen und wird durch den oder die IT-SIBE bei ihrer Aufsicht unterstützt.

[3] Der oder dem IT-SIBE obliegt die Aufsicht über die Gewährleistung der Informationssicherheit bei Tätigkeiten, bei denen keine Personendaten bearbeitet werden. Sie oder er kann zur Mitarbeit in beratender Funktion in ICT-Projekten eingeladen werden.

[4] ISDS-relevante Weisungen der Stellen, für die diese Verordnung gilt (Art. 2 Abs. 2), sind spätestens eine Woche vor ihrem Erlass der kantonalen Datenschutzaufsichtsstelle und der oder dem IT-SIBE informationshalber zuzustellen. In ISDS-relevante Rechtsetzungsvorhaben sind die kantonale Datenschutzaufsichtsstelle und die oder der IT-SIBE in geeigneter Weise einzubeziehen.

Art. 11 *IT-SIVE*

[1] Die Direktionen und die Staatskanzlei bezeichnen eine Informationssicherheitsverantwortliche oder einen Informationssicherheitsverantwortlichen (IT-SIVE) als hauptsächliche Kontaktstelle der oder des IT-SIBE.

Art. 12 *Weisungen des Amtes für Informatik und Organisation*

[1] Das Amt für Informatik und Organisation (KAIO) erlässt nach Konsultation der Direktionen, der Staatskanzlei und der kantonalen Datenschutzaufsichtsstelle und der kantonalen Informatikkonferenz (KIK) die erforderlichen Ausführungsweisungen, namentlich über

a die bei ICT-Vorhaben durchzuführende ISDS-Analyse und Schutzbedarfsklassifizierung,
b das bei ICT-Vorhaben zu erstellende ISDS-Konzept,
c den zu beachtenden ISDS-Grundschutz,
d allgemeine ISDS-Geschäftsbedingungen des Kantons (AGB ISDS), die für ICT-Vorhaben verbindlich einzuhalten bzw. vorzugeben sind.

[2] Die allgemeinen ISDS-Geschäftsbedingungen gemäss Absatz 1 Buchstabe d können vorsehen, dass vertragliche Regelungen die im Einzelfall gestützt auf Absatz 1 Buchstaben a bis c erarbeiteten ISDS-Grundlagen enthalten müssen.

[3] Das KAIO stellt geeignete Hilfsmittel (Erläuterungen, Checklisten usw.) zur Verfügung und sorgt für ein angemessenes Beratungs- und Schulungsangebot.

Art. 13 *Inkrafttreten*

[1] Diese Verordnung tritt am 1. April 2011 in Kraft.

Bern, 3. Januar 2011 Die Finanzdirektorin:Simon

Änderungstabelle - nach Beschluss

Beschluss	Inkrafttreten	Element	Änderung	BAG-Fundstelle
03.01.2011	01.04.2011	Erlass	Erstfassung	11-12

Änderungstabelle - nach Artikel

Element	Beschluss	Inkrafttreten	Änderung	BAG-Fundstelle
Erlass	03.01.2011	01.04.2011	Erstfassung	11-12