Verordnung über die Informations- und Datensicherheit (IDSV)

vom 09.09.2026 (Stand 01.11.2026)

Der Regierungsrat des Kantons Bern,

gestützt auf Artikel 8 Absatz 4, Artikel 11, 15, 23 Absatz 2 und Artikel 31 Absatz 1 und 2 des Gesetzes vom 12. Juni 2025 über die Informations- und Cybersicherheit (ICSG)[1)] sowie auf Artikel 10 Absatz 2 und Artikel 57 des Kantonalen Datenschutzgesetzes vom 3. Dezember 2025 (KDSG)[2)],

auf Antrag der Finanzdirektion,

beschliesst:

1 Allgemeine Bestimmungen

Art. 1 *Gegenstand*

[1] Diese Verordnung regelt die Aufgaben, Verantwortlichkeiten und Kompetenzen sowie die Verfahren zur Gewährleistung der Informationssicherheit (Art. 4 Abs. 1 Bst. a ICSG) und der Datensicherheit (Art. 10 Abs. 1 KDSG) der Behörden nach Artikel 2.

Art. 2 *Geltungsbereich*

[1] Diese Verordnung gilt für die kantonalen Behörden nach Artikel 3 Absatz 1 Buchstabe h.

[2] Für die anderen Behörden gelten nur die Bestimmungen nach Abschnitt 1 und 2 sowie Artikel 41, und nur soweit die Behörden:

a klassifizierte Informationen des Kantons oder des Bundes bearbeiten,
b ICT-Mittel des Kantons oder des Bundes einsetzen, oder
c Personendaten nach Artikel 2 Absatz 1 KDSG bearbeiten.

1) BSG 152.09
2) BSG 152.04

* Änderungstabellen am Schluss des Erlasses

Art. 3 *Begriffe*

[1] In dieser Verordnung bedeuten:

a Schutzniveau: Die Wirkung der Schutzmassnahmen, die je nach Schutzbedarf der Schutzobjekte umgesetzt werden,
b Schutzobjekte: Informationen, Personendaten oder ICT-Mittel,
c Sicherheitsvorfall: Ein Ereignis, das die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Bearbeitung von Informationen oder Personendaten oder die Sicherheit von ICT-Mitteln beeinträchtigt,
d Cyberangriff: Ein Sicherheitsvorfall, der absichtlich ausgelöst wird,
e Schwachstelle: Eine Schwäche oder ein Fehler eines ICT-Mittels, die oder der das Potenzial hat, einen Sicherheitsvorfall zu ermöglichen,
f Sicherheitsverantwortliche oder Sicherheitsverantwortlicher (SIVE, Art. 36): Die oberste Führungsperson einer kantonalen Behörde, welche die Gesamtverantwortung für die Informations- und Datensicherheit ihrer Behörde trägt,
g Sicherheitsbeauftragte oder Sicherheitsbeauftragter (SIBE, Art. 37): Die Sicherheitsfachperson einer kantonalen Behörde, welche die oder den SIVE berät und unterstützt,
h Kantonale Behörden: Der Grosse Rat, die kantonale Datenschutzbehörde, die Finanzkontrolle, der Regierungsrat, die Kantonsverwaltung ohne die teilautonomen Organisationen nach Artikel 3 Absatz 1 der Verordnung vom 27 November 2002 über die Organisation und die Aufgaben der Bildungs- und Kulturdirektion (Organisationsverordnung BKD, OrV BKD[3)]), die Gerichtsbehörden sowie die Staatsanwaltschaft.

2 Grundsätze

Art. 4 *Führungsverantwortung*

[1] Die oberste Führung einer Behörde

a sorgt dafür, dass die Informations- und Datensicherheit nach den geltenden Vorschriften sowie dem Stand der Technik organisiert, umgesetzt und überprüft wird,
b akzeptiert nachweisbar die nach der Umsetzung von Schutzmassnahmen verbleibenden Restrisiken in ihrem Verantwortungsbereich.

[2] Die Vorgesetzten jeder Stufe sorgen für die Schulung bei Stellenantritt und die periodische Sensibilisierung sowie Weiterbildung ihrer Mitarbeiterinnen und Mitarbeiter.

[3)] BSG 152.221.181

[3] Die Vorgesetzten jeder Stufe sowie die Mitarbeiterinnen und Mitarbeiter sind für den vorschriftskonformen Umgang mit Schutzobjekten verantwortlich.

[4] Die Verantwortung verbleibt auch bei der Bearbeitung der Informationen oder Personendaten sowie beim Betrieb der ICT-Mittel durch beauftragte Dritte bei der Behörde.

Art. 5 *Präventive Schutzmassnahmen*

[1] Die Behörden gewährleisten die Ziele der Informations- und Datensicherheit mit folgenden, präventiven und risikoangemessenen Schutzmassnahmen:

a Vertraulichkeit durch Zugriffs-, Zugangs- und Benutzerkontrolle,
b Verfügbarkeit und Integrität durch
  1. Datenträger- und Transportkontrolle,
  2. Möglichkeit zur Wiederherstellung,
  3. automatische Meldung von und Schutz vor Fehlfunktionen,
  4. aktuelle Systemsicherheit,
c Nachvollziehbarkeit bei Informationen ab der Klassifizierung «INTERN» und bei Personendaten durch
  1. Eingabekontrolle,
  2. Bekanntgabekontrolle,
  3. rasche Erkennung und Behebung der Folgen von Sicherheitsvorfällen.

Art. 6 *Protokollierung bei digitaler Bearbeitung von Personendaten*

[1] Wenn Behörden und beauftragte Dritte Personendaten digital bearbeiten, die risikoangemessene Datensicherheit trotz präventiver Schutzmassnahmen aber nicht gewährleistet ist, protokollieren sie das Speichern, Verändern, Löschen und Vernichten der Personendaten.

[2] Wenn sie besonders schützenswerte Personendaten digital bearbeiten oder ein Profiling mit hohem Risiko nach Artikel 2 Absatz 1 Buchstabe h KDSG durchführen, die risikoangemessene Datensicherheit trotz präventiver Schutzmassnahmen aber nicht gewährleistet ist, protokollieren sie zusätzlich das Zugreifen auf die Personendaten sowie deren Bekanntgeben.

[3] Die Protokolle müssen während mindestens eines halben Jahres aufbewahrt werden.

Art. 7 *Meldung von Sicherheitsvorfällen, Schwachstellen und Cyberangriffen*

[1] Entdecken die Behörden oder deren beauftragten Dritten Sicherheitsvorfälle, Schwachstellen oder Cyberangriffe, welche die Aufgabenerfüllung oder die Informations- oder Datensicherheit wesentlich gefährden, ergreifen sie unverzüglich die erforderlichen Sofortmassnahmen und erstatten Meldung über die Plattform nach Absatz 4.

[2] Cyberangriffe, Sicherheitsvorfälle oder Schwachstellen sind innert 24 Stunden nach Entdeckung zu melden. Betreffen sie allein Personendaten, sind sie innert 72 Stunden zu melden (Art. 26 Abs. 1 KDSG).

[3] Wenn nach Artikel 27 KDSG geboten, hat die Behörde der durch die Verletzung der Datensicherheit betroffenen Person in einfacher Sprache mindestens die folgenden Angaben mitzuteilen:

a Behörde sowie Namen und Kontaktangaben der meldenden Person,
b Beschreibung der Beeinträchtigung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Personendaten,
c getroffene und geplante Massnahmen zur Wiederherstellung und künftigen Sicherstellung der Datensicherheit.

[4] Die Beratungsstelle Informations- und Datensicherheit (Beratungsstelle IDS)

a stellt eine Plattform zur Erfüllung der Meldepflichten zur Verfügung,
b legt die zu meldenden Angaben nach den gesetzlichen Vorgaben fest,
c kann die Meldungen einsehen und zur Erfüllung ihrer eigenen Aufgaben nutzen,
d stellt sicher, dass die Meldungen an das Bundesamt für Cybersicherheit (BACS) weitergeleitet werden.

Art. 8 *Schutzbedarfsanalyse und ISDS-Konzept anderer Behörden*

[1] Die anderen Behörden nach Artikel 2 Absatz 2 führen die Risikoanalyse und nötigenfalls die Datenschutzfolgeabschätzung (Art. 18 und 19 KDSG) durch, indem sie die Instrumente der Schutzbedarfsanalyse (Art. 13) sowie des Informationssicherheits- und Datenschutzkonzepts (ISDS-Konzept, Art. 16) den Risiken der Behörden angemessen und unter Berücksichtigung der Empfehlungen ihrer Datenschutzbehörde anwenden.

Art. 9 *Vorabkontrolle*

[1] Eine wesentliche Änderung im Sinne von Artikel 20 Absatz 2 KDSG und damit die Pflicht zur Vorabkontrolle liegt vor, wenn

a die Mittel oder der Zweck der Datenbearbeitung in erheblicher Weise ändern oder

b die Änderung für sich allein die Voraussetzungen für eine Vorabkontrolle erfüllt.

[2] Die Änderung des Umfangs einer Datenbearbeitung ist keine wesentliche Änderung, ausser wenn damit die Schwelle nach Absatz 3 Buchstabe b überschritten wird.

[3] Keiner Vorabkontrolle bedarf es, wenn

a die ICT-Mittel oder -Dienstleistungen nach Artikel 13 des Bundesgesetzes vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG)[4)] hinsichtlich der Informations- und Datensicherheit zertifiziert sind oder

b Personendaten von weniger als 1000 Personen bearbeitet werden.

[4] Die kantonale Datenschutzbehörde

a legt fest, welche Angaben die ihr zur Vorabkontrolle unterbreiteten Unterlagen enthalten müssen,

b kann Vorlagen als verbindlich erklären, wobei sie sich an den Vorgaben der Konferenz digitale Verwaltung und ICT (KDI) nach Artikel 18 der Verordnung vom 11. Januar 2023 über die digitale Verwaltung (DVV)[5)] orientiert.

Art. 10 *Betrieb von ICT-Mitteln*

[1] Die Behörden überwachen die Nutzung der von ihnen verantworteten ICT-Mittel und durchsuchen sie risikoangemessen nach technischen Bedrohungen und Schwachstellen.

[2] Sie stellen sicher, dass die Verantwortlichkeiten und Schutzmassnahmen für die Informations- und Datensicherheit beim Betrieb von ICT-Mitteln in den Verträgen mit beauftragten Dritten geregelt und umgesetzt werden.

---

4) SR 235.1

5) BSG 109.111

Art. 11 *Restriktive Berechtigungen*

[1] Die Behörden sorgen im Rahmen ihrer Zugriffs-, Zutritts- und Benutzerkontrollen nach Artikel 5 Absatz 1 Buchstabe a dafür, dass die Berechtigungen entzogen werden, sobald eine Anstellung oder ein Vertrag endet oder die Aufgabe erfüllt ist.

[2] Berechtigungen dürfen ohne Vorankündigung entzogen werden, wenn konkrete Anhaltspunkte für eine Gefährdung von Schutzobjekten vorliegen.

[3] Die Behörden prüfen periodisch und risikoorientiert die Berechtigungen für die in ihrer Verantwortung betriebenen ICT-Mittel.

Art. 12 *Zusammenarbeit zwischen den Behörden*

[1] Die Behörden tragen durch die Zusammenarbeit und den Informationsaustausch mit den anderen Behörden und Kantonen, dem Bund sowie der Wissenschaft zur Verbesserung der Informations- und Datensicherheit des Kantons bei.

[2] Sie können sich gegenseitig Personendaten bekanntgeben, wenn dies der Informations- oder Datensicherheit dient.

3 Schutzmassnahmen kantonaler Behörden

3.1 Sicherheitsverfahren bei ICT-Mitteln

Art. 13 *Schutzbedarfsanalyse*

[1] Die kantonalen Behörden

a ermitteln den Schutzbedarf ihrer ICT-Mittel anhand deren Relevanz für das betriebliche Kontinuitätsmanagement sowie der damit bearbeiteten Informationen und Personendaten,

b weisen den Schutzbedarf in der Schutzbedarfs- bzw. Risikoanalyse (nachfolgend Schutzbedarfsanalyse) aus.

[2] ICT-Mittel ohne Schutzbedarfsanalyse dürfen nicht in Betrieb genommen werden.

Art. 14 *Grundschutz*

[1] Die kantonalen Behörden stellen den Grundschutz für die Informations- und Datensicherheit des Kantons (Grundschutz BE) gemäss Weisung der KDI (Art. 35) sicher.

Art. 15 *Einstufen in Schutzniveaus*

[1] Die kantonalen Behörden stufen die Schutzobjekte aufgrund ihrer Bedeutung und Bedrohung in die Schutzniveaus nach Anhang 1 ein (Schutzbedarf).

[2] Die Schutzniveaus 0 und 1 werden durch den Grundschutz BE gewährleistet.

Art. 16 *ISDS-Konzept*

[1] Ergibt die Schutzbedarfsanalyse, dass ein ICT-Mittel den Grundschutz BE nicht erfüllt oder erhöhte Sicherheitsanforderungen erfüllen muss, so erstellen die kantonalen Behörden ein Informationssicherheits- und Datenschutzkonzept bzw. eine Datenschutzfolgenabschätzung (nachfolgend ISDS-Konzept) mit folgendem Inhalt:

a Risiken, die infolge nicht oder nur teilweise erfüllter Grundschutzanforderungen bestehen,
b besondere, über den Grundschutz hinausgehende Schutzmassnahmen,
c verbleibende Restrisiken.

[2] Erhöhte Anforderungen an die Informations- und Datensicherheit bestehen insbesondere, wenn

a eine Wiederherstellung der Schutzobjekte mit erheblichen Problemen oder Kosten verbunden ist,
b die bearbeiteten Informationen oder Personendaten besonderen gesetzlichen oder vertraglichen Geheimhaltungsvorschriften unterliegen,
c eine Datensicherheitsverletzung für die Betroffenen spürbar nachteilige Folgen hat, insbesondere bei besonders schützenswerten Personendaten,
d die bearbeiteten Informationen als «VERTRAULICH» oder «GEHEIM» klassifiziert sind,
e dem ICT-Mittel die Einstufung «Hoher Schutz» oder «Sehr hoher Schutz» zugeordnet wird.

[3] Die kantonalen Behörden bewahren das ISDS-Konzept nach dem Ende der Informations- oder Datenbearbeitung mindestens zwei Jahre auf.

Art. 17 *Beauftragte Dritte*

[1] Die kantonalen Behörden beurteilen mit ihren Schutzbedarfsanalysen die Risiken für ihre Schutzobjekte, welche aus deren Bearbeitung durch beauftragte Dritte und der Abhängigkeit von diesen entstehen.

[2] Sie vereinbaren mit den beauftragten Dritten die von den Weisungen der KDI vorgegebenen Vertragsinhalte, zusammen mit den weitergehenden Schutzmassnahmen gemäss ISDS-Konzept.

Art. 18 *Bestätigung der Informations- und Datensicherheit*

[1] Mit der Genehmigung des ISDS-Konzepts bestätigt die oberste Führung bzw. die oder der SIVE die Informations- und Datensicherheit des ICT-Mittels und akzeptiert allfällige Restrisiken.

3.2 Management der Informations- und Datensicherheit

Art. 19 *Restrisiken und aktuelle Bedrohungen*

[1] Die SIVE können ihrer jeweils vorgesetzten kantonalen Behörde besonders bedeutsame Restrisiken zum Akzeptieren vorlegen.

[2] Die Beratungsstelle IDS

a informiert die kantonalen Behörden regelmässig über aktuelle Bedrohungen und Schwachstellen,
b empfiehlt bei Bedarf Schutzmassnahmen zur Risikominderung.

Art. 20 *Informationssicherheits-Managementsystem*

[1] Die KDI stellt das Management der Informationssicherheitsrisiken der Direktionen, der Staatskanzlei sowie der Gerichtsbehörden und der Staatsanwaltschaft nach Artikel 5 Absatz 2 ICSG mit einem Informationssicherheits-Managementsystems (ISMS) sicher.

[2] Die KDI lässt das ISMS mindestens alle drei Jahre von einer unabhängigen Stelle überprüfen und sorgt für dessen kontinuierliche Verbesserung.

Art. 21 *Inventar der Schutzobjekte*

[1] Die kantonalen Behörden inventarisieren und aktualisieren in ihrem Verantwortungsbereich:

a Sammlungen von Informationen oder Personendaten ab Schutzniveau 1,
b ICT-Mittel,
c kritische und meldepflichtige Infrastrukturen nach Artikel 74b des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit (Informationssicherheitsgesetz, ISG[6)]),
d Sicherheitszonen.

[2] Die KDI legt die zu führenden Angaben zu den Schutzobjekten fest.

[6)] SR 128

Art. 22 *Schutzmassnahmen bei Nutzung von Schutzobjekten durch Dritte*

[1] Stellen kantonale Behörden anderen Behörden oder Privaten kantonale Schutzobjekte zur Verfügung, legen die kantonalen Behörden soweit erforderlich durch Weisung, Verfügung oder Vertrag die umzusetzenden Schutzmassnahmen fest.

[2] Bundesbehörden können für ihre Schutzobjekte Vorschriften nach Absatz 1 erlassen.

Art. 23 *Ausnahmen von den Vorschriften*

[1] Kann oder will eine kantonale Behörde für ein Schutzobjekt die vorgeschriebene Schutzmassnahme nicht umsetzen, beantragt sie eine Ausnahmebewilligung der oder des SIBE der KDI (SIBE KDI). Die oder der SIBE KDI hört vorgängig die Behörden an, deren Zuständigkeitsbereich für die Informations- und Datensicherheit die Ausnahme betrifft.

[2] Betrifft die Ausnahme allein den Verantwortungsbereich der antragstellenden kantonalen Behörde, so kann die oder der SIBE KDI die Kompetenz zur Ausnahmebewilligung dieser Behörde übertragen.

[3] Die Beratungsstelle IDS führt ein Verzeichnis der Ausnahmebewilligungen.

Art. 24 *Unterstützung bei Sicherheitsvorfällen*

[1] Die Beratungsstelle IDS unterstützt die betroffene kantonale Behörde auf deren Antrag und im Rahmen ihrer Kapazität bei der Bewältigung von Sicherheitsvorfällen oder Schwachstellen.

Art. 25 *Kontrollen und Audits*

[1] Die SIVE DIR nach Artikel 36 Absatz 1 beschliessen auf Antrag ihrer SIBE sowie in Absprache mit der Beratungsstelle IDS einen jährlichen Kontroll- und Auditplan für die Organisationseinheiten und beauftragten Dritten in ihrem Verantwortungsbereich.

[2] Die Beratungsstelle IDS

a koordiniert ihre Kontroll- und Auditpläne mit der kantonalen Datenschutzbehörde sowie der Finanzkontrolle,

b kann mit Zustimmung der SIVE DIR Kontrollen und Audits durchführen oder Dritte damit beauftragen.

Art. 26 *Berichterstattung*

[1] Die SIBE DIR nach Artikel 37 Absatz 2 Buchstabe a erstatten der oder dem SIBE KDI jährlich Bericht über die Umsetzung und Wirksamkeit der Informations- und Datensicherheit in ihrem Zuständigkeitsbereich.

[2] Die oder der SIBE KDI

a erstattet in Zusammenarbeit mit der Fachgruppe IDS der KDI jährlich Bericht über die Umsetzung und Wirksamkeit der Informations- und Datensicherheit der kantonalen Behörden,
b zieht dazu auch die Audits der kantonalen Behörden und der Aufsichtsbehörden heran.

[3] Die KDI genehmigt den Bericht und beschliesst nötigenfalls Verbesserungsmassnahmen.

[4] Der Bericht ist mindestens als «VERTRAULICH» zu klassifizieren.

3.3 Klassifizierung von Informationen

Art. 27 *Klassifizierungskataloge*

[1] Die SIVE DIR legen auf Antrag ihrer SIBE je in einem Klassifizierungskatalog fest, wie die in ihrem Zuständigkeitsbereich häufig bearbeiteten Informationen zu klassifizieren sind und wie lange die Klassifizierung dauern soll.

[2] Die oder der SIBE KDI überprüft die Klassifizierungskataloge der SIVE DIR und gibt ihnen bei Bedarf eine Empfehlung ab.

[3] Die KDI beschliesst auf Antrag der oder des SIBE KDI und nach Konsultation der SIVE DIR einen Klassifizierungskatalog für die Direktionen und die Staatskanzlei.

Art. 28 *Klassifizierende und Ausführungsweisungen*

[1] Folgende Personen der kantonalen Behörden sind für die Klassifizierung und Entklassifizierung von Informationen, die nicht in den Klassifizierungskatalogen aufgeführt sind, verantwortlich:

a die Mitarbeiterinnen und Mitarbeiter, welche die Informationen erstellen oder verändern,
b die auftraggebende Person bei der Bearbeitung von Informationen durch beauftragte Dritte.

[2] Die Mitarbeiterinnen und Mitarbeiter der kantonalen Behörden sind für die Kennzeichnung der Informationsträger, die sie erstellen, oder der Informationen, die sie mündlich mitteilen, verantwortlich.

[3] Die KDI erlässt auf Antrag der oder des SIBE KDI eine Weisung über die Bearbeitung von klassifizierten Informationen. Sie regelt im Einvernehmen mit dem Amt für Kommunikation auch die Gestaltung von Klassifizierungsvermerken.

Art. 29 *Klassifizierung «INTERN»*

[1] Als «INTERN» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen nach Artikel 1 Absatz 2 Buchstaben a und b ICSG wie folgt beeinträchtigen kann:

a Ein wichtiger Geschäftsprozess des Regierungsrates oder der kantonalen Behörden ist erschwert.
b Die Durchführung von Einsätzen der Strafverfolgungsbehörden oder anderer Sicherheitsorgane des Kantons ist erschwert.
c Einzelne Personen sind körperlich verletzt.
d Der Schutz vor Naturereignissen oder die Sicherung der Infrastruktur zum Schutz vor Naturereignissen ist mittelbar gefährdet.
e Der Kanton ist politisch oder in seinen wirtschaftlichen Interessen beeinträchtigt.
f Die Beziehungen zum Bund und zu den Kantonen oder zwischen den Kantonen sind gestört.

Art. 30 *Klassifizierung «VERTRAULICH»*

[1] Als «VERTRAULICH» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen nach Artikel 1 Absatz 2 Buchstaben a und b ICSG wie folgt erheblich beeinträchtigen kann:

a Die Entscheidungs- oder Handlungsfähigkeit des Regierungsrates, des Grossen Rates oder mehrerer Behörden ist über mehrere Tage erschwert.
b Die zielkonforme Durchführung von Operationen der Strafverfolgungsbehörden oder anderer Sicherheitsorgane des Kantons ist gefährdet.
c Die operativen Mittel und Methoden der Strafverfolgungsbehörden des Kantons oder die Identität oder der Aufenthalt von Quellen und exponierten Personen sind offengelegt.
d Die Sicherheit der Bevölkerung ist über mehrere Tage gefährdet oder einzelne Personen oder Personengruppen kommen zu Tode.
e Der Schutz vor Hochwasser oder die Sicherung der Infrastruktur zum Schutz vor Hochwasser ist gefährdet.

f Die wirtschaftliche Versorgung des Kantons, auch von Teilen davon, oder der Betrieb von kritischen Infrastrukturen nach Artikel 74b ISG ist erschwert.
g Der Kanton ist politisch oder in seinen wirtschaftlichen Interessen erheblich beeinträchtigt.
h Die Beziehungen zu einem anderen Kanton oder einer interkantonalen Organisation sind abgebrochen.

Art. 31 *Klassifizierung «GEHEIM»*

[1] Als «GEHEIM» werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte die öffentlichen Interessen nach Artikel 1 Absatz 2 Buchstaben a und b ICSG wie folgt schwerwiegend beeinträchtigen kann:

a Die Entscheidungs- oder Handlungsfähigkeit des Regierungsrates, des Grossen Rates oder mehrerer Behörden ist über mehrere Tage verunmöglicht oder über Wochen erschwert.
b Die Durchführung von strategisch bedeutsamen Operationen der Strafverfolgungsbehörden oder anderer Sicherheitsorgane des Kantons ist gefährdet oder über Tage in hohem Mass erschwert.
c Die strategischen Mittel und Methoden der Strafverfolgungsbehörden des Kantons oder die Identität oder der Aufenthalt von strategischen Quellen oder besonders exponierten Personen sind offengelegt.
d Die Sicherheit der Bevölkerung ist über Wochen in besonders hohem Mass gefährdet oder eine grosse Anzahl Personen kommt zu Tode.
e Der Schutz vor Hochwasser oder die Sicherung der Infrastruktur zum Schutz vor Hochwasser ist in hohem Mass gefährdet.
f Die wirtschaftliche Versorgung des Kantons, auch von Teilen davon, oder der Betrieb von kritischen Infrastrukturen ist in hohem Mass gefährdet.
g Der Kanton leidet in hohem Mass unter politischen oder wirtschaftlichen Massnahmen Dritter.

Art. 32 *Entklassifizierung und Entfallen der Klassifizierung*

[1] Die klassifizierende Behörde bzw. deren nach Artikel 28 Absatz 1 Verantwortlichen entklassifizieren Informationen, wenn die Klassifizierungsvoraussetzungen nicht mehr vorliegen.

[2] Sie überprüft dies namentlich

a beim Abschluss des Geschäfts,
b bei Zugangsbegehren zu behördlichen Informationen.

[3] Die Klassifizierung von Archivgut entfällt mit Ablauf der archivrechtlichen Schutzfrist.

3.4 Einstufung von ICT-Mitteln

Art. 33 *«Grundschutz», «Hoher Schutz» und «Sehr hoher Schutz»*

[1] Die kantonalen Behörden stufen ihre ICT-Mittel gestützt auf die Schutzbedarfsanalyse wie folgt ein:

a «Hoher Schutz», wenn eine Verletzung der Informations- und Datensicherheit eines der folgenden Risiken birgt:
   1. Ein Ausfall des ICT-Mittels erschwert die Erfüllung von kritischen Aufgaben erheblich.
   2. Eine Beeinträchtigung, welche die Klassifizierungsstufe «VERTRAULICH» erfordert.
   3. Es droht ein geschätzter Schaden von 20 bis 100 Millionen Franken.
   4. Es besteht für die betroffene Person ein hohes Risiko nach Artikel 18 KDSG.

b «Sehr hoher Schutz», wenn eine Verletzung der Informations- und Datensicherheit eines der folgenden Risiken birgt:
   1. Ein Ausfall des ICT-Mittels verunmöglicht die Erfüllung von kritischen Aufgaben.
   2. Eine Beeinträchtigung, welche die Klassifizierungsstufe «GEHEIM» erfordert.
   3. Es droht ein geschätzter Schaden von über 100 Millionen Franken.
   4. Es besteht für die betroffenen Personen ein Risiko für Leib, Leben oder Freiheit.

c «Grundschutz» für die übrigen ICT-Mittel.

[2] Sie haben bei ICT-Mitteln der Einstufung «Hoher Schutz» und «Sehr hoher Schutz» das Sicherheitsverfahren bei Änderungen des ICT-Mittels, der Bedrohung, der Technologie, der Aufgaben oder der Organisationsverhältnisse, spätestens aber zwei Jahre nach der letzten Durchführung zu wiederholen.

3.5 Zu prüfende Personen

Art. 34

[1] Der Regierungsrat beschliesst auf Antrag der Finanzdirektion und nach Konsultation der Konferenz der Generalsekretärinnen und -sekretäre (GSK), für welche vom Regierungsrat zu besetzenden Funktionen oder beauftragten Personen welche Personensicherheitsprüfung erfolgt.

[2] Die GSK beschliesst auf Antrag der KDI, für welche weiteren Funktionen und Beauftragten der kantonalen Verwaltung welche Personensicherheitsprüfung erfolgt.

[3] Die Listen nach den Beschlüssen nach Absatz 1 und 2 sind nicht öffentlich.

4 Sicherheitsorganisation

Art. 35 *Konferenz digitale Verwaltung und ICT*

[1] Die KDI erlässt für die kantonalen Behörden konkretisierende Weisungen. Sie orientiert sich dabei an internationalen Standards und solchen des Bundes, soweit diese für den Kanton risikoangemessen sind.

[2] Sie führt eine Liste der neuen Technologien, die mit hohen Risiken verbunden sind (Art. 18 Abs. 2 KDSG).

[3] Sind von den Weisungen auch die Einwohner-, Burger- oder Kirchgemeinden betroffen, werden diese nach Artikel 22 DVG zur Konsultation eingeladen.

[4] Die KDI kann den Erlass von Weisungen von untergeordneter Bedeutung oder vorwiegend technischer Natur an die Fachgruppe Informations- und Datensicherheit (Fachgruppe IDS) delegieren.

Art. 36 *Sicherheitsverantwortliche*

[1] Die SIVE DIR sind für

a den Grossen Rat und die Direktionen: die Generalsekretärin oder der Generalsekretär,
b die Staatskanzlei: die Staatsschreiberin oder der Staatsschreiber,
c die Datenschutzbehörde: die oder der Beauftragte für Datenschutz,
d die Finanzkontrolle: die Vorsteherin oder der Vorsteher,
e die ICT-Grundversorgung und die Konzernapplikationen des Amtes für Informatik und Organisation (KAIO): die Vorsteherin oder der Vorsteher des KAIO,
f die Gerichtsbehörden und die Staatsanwaltschaft: die von ihnen bezeichnete Führungsperson.

[2] Die SIVE Amt sind für die Ämter oder die ihnen gleichgestellten Organisationseinheiten die Amtsvorsteherinnen und -vorsteher.

[3] Die Personen nach Absatz 1 und 2 können die Rolle sowie die Aufgaben und Kompetenzen der oder des SIVE einer ihnen direkt unterstellten Funktion delegieren.

[4] Die SIVE DIR und Amt

a treffen alle Entscheide, welche die Informations- und Datensicherheit in ihrem Zuständigkeitsbereich massgeblich beeinflussen, insbesondere betreffend Organisation, Prozesse, Risikoakzeptanz und Sicherheitsziele,
b bezeichnen ihre SIBE nach Artikel 37 sowie deren Stellvertretung.

Art. 37 *Sicherheitsbeauftragte*

[1] Die Leiterin oder der Leiter der Beratungsstelle IDS ist die oder der Sicherheitsbeauftrage der KDI (SIBE KDI).

[2] Eine oder ein SIBE kann

a die Rollen SIBE DIR und SIBE Amt gleichzeitig innehaben,
b diese Rollen für mehrere Organisationseinheiten innehaben.

[3] Die SIBE

a sorgen insbesondere für die Umsetzung der Vorschriften über die Informations- und Datensicherheit,
b sind zentrale Anlaufstelle ihrer Organisationseinheit für Fragen zur Informations- und Datensicherheit und
c beraten und unterstützen die zuständigen Personen und Stellen bei der Erfüllung ihrer Aufgaben und Pflichten.

[4] Die KDI kann die Aufgaben, Kompetenzen und Verantwortlichkeiten der SIBE KDI, DIR und Amt durch Weisung konkretisieren.

Art. 38 *Fachgruppe Informations- und Datensicherheit*

[1] Der Fachgruppe Informations- und Datensicherheit (Fachgruppe IDS) gehören mindestens die oder der SIBE KDI, die SIBE DIR und die oder der SIBE Kantonspolizei an.

[2] Die Fachgruppe IDS sorgt insbesondere für die direktionsübergreifende Koordination der Informationssicherheit.

Art. 39 *Beratungsstelle Informations- und Datensicherheit*

[1] Die Beratungsstelle IDS

a ist die zentrale Anlaufstelle der kantonalen Behörden für Fragen zur Informations- und Datensicherheit,
b berät und unterstützt die kantonalen Behörden bei der Erfüllung ihrer Aufgaben und Pflichten.

[2] Die Beratungsstelle IDS ist Teil des KAIO.

[3] Die KDI kann die Aufgaben, Kompetenzen und Verantwortlichkeiten der Beratungsstelle IDS durch Weisung konkretisieren.

Art. 40 *Belohnung für das Erkennen und Melden von Schwachstellen*

[1] Die Beratungsstelle IDS nimmt Hinweise Dritter auf Schwachstellen bei ICT-Mitteln des Kantons entgegen und leitet sie an die verantwortlichen Behörden weiter.

[2] Sie kann für Hinweise, die zur Behebung von Schwachstellen oder zur Reduktion von Sicherheitsrisiken führen, eine Belohnung ausrichten.

[3] Der Betrag der Belohnung

a richtet sich nach dem Umfang, in dem das Sicherheitsrisiko aufgrund des Hinweises reduziert wird,
b beläuft sich auf höchstens 10'000 Franken pro Hinweis.

[4] Auf die Belohnung besteht kein Rechtsanspruch.

5 Übergangs- und Schlussbestimmungen

Art. 41 *Übergangsbestimmungen*

[1] Das ISMS muss innert zwei Jahren nach Inkrafttreten dieser Verordnung in Betrieb sein.

[2] Das Inventar der Schutzobjekte sowie der Klassifizierungskatalog sind innert eines Jahres nach Inkrafttreten dieser Verordnung zu erstellen.

[3] Die betreffende und zuständige Person sorgt dafür, dass bisher nicht klassifizierte Informationen nach Inkrafttreten dieser Verordnung bei erstmaliger Bearbeitung klassifiziert werden.

[4] Für jedes ICT-Mittel, das beim Inkrafttreten dieser Verordnung über keine aktuelle Schutzbedarfsanalyse und, soweit erforderlich, über kein ISDS-Konzept verfügt, gelten folgende Übergangsfristen:

a Kantonale Behörden nehmen innert eines Jahres nach Inkrafttreten dieser Verordnung eine Schutzbedarfsanalyse vor und erstellen nötigenfalls innert zwei Jahren ein ISDS-Konzept.
b Andere Behörden nehmen innert zwei Jahren nach Inkrafttreten dieser Verordnung eine Schutzbedarfsanalyse vor und erstellen nötigenfalls innert drei Jahren ein ISDS-Konzept.

[5] Die Behörden passen bestehende ICT-Mittel und Verträge bei der nächsten Neubeschaffung oder Änderung, spätestens aber bis zum 1. Oktober 2030 an ihre Grundschutzanforderungen an.

[6] Die im Zeitpunkt des Inkrafttretens dieser Verordnung bei einer kommunalen Datenschutzbehörde hängigen Vorabkontrollen werden von der betreffenden Datenschutzbehörde bis zum Abschluss geführt.

[7] Für die Informations- und Datensicherheit von Regierungsratsgeschäften bleibt die Verordnung vom 13. März 2013 über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV)[7)] bis zu deren Anpassung an diese Verordnung anwendbar.

Art. 42 *Änderung von Erlassen*

[1] Folgende Erlasse werden geändert:

a Verordnung vom 11. Januar 2023 über die digitale Verwaltung (DVV)[8)],
b Verordnung vom 4. November 1998 über die Ausgleichskasse des Kantons Bern und ihre Zweigstellen (AKBV)[9)],
c Verordnung vom 20. Mai 2020 über die Datenbearbeitung im Asyl-, Flüchtlings- und Ausländerbereich (DAFAV)[10)].

Art. 43 *Aufhebung eines Erlasses*

[1] Die Direktionsverordnung vom 3. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV)[11)] wird aufgehoben.

Art. 44 *Inkrafttreten*

[1] Diese Verordnung tritt am 1. November 2026 in Kraft.

Bern, 9. September 2026

Im Namen des Regierungsrates
Der Präsident: Schnegg
Der Staatsschreiber: Auer

7) BSG 152.17
8) BSG 109.111
9) BSG 841.111
10) BSG 861.112
11) BSG 152.040.2

Änderungstabelle - nach Beschluss

Beschluss	Inkrafttreten	Element	Änderung	BAG-Fundstelle
09.09.2026	01.11.2026	Erlass	Erstfassung	26-051

Änderungstabelle - nach Artikel

Element	Beschluss	Inkrafttreten	Änderung	BAG-Fundstelle
Erlass	09.09.2026	01.11.2026	Erstfassung	26-051

Anhang 1 zu Artikel 15 Absatz 1

(Stand 01.11.2026)

Schutzobjekte, Einstufung und Schutzniveaus

ICSG		IDSV	KDSG
Schutz der Interessen des Staates		**Massnahmen für die Informations- und Datensicherheit**	**Schutz der Interessen von Personen**
ICT-Mittel	Informationen	Schutzmassnahmen nach Stand der Technik	Personendaten
Sehr hoher Schutz	GEHEIM	Schutzniveau 3	Personendaten als grosse Gefahr für die Sicherheit Einzelner (Leib, Leben, Freiheit)
Hoher Schutz	VERTRAULICH	Schutzniveau 2	Besonders schützenswerte Personendaten und Personendaten mit besonderer Geheimhaltung (Berufs-, Steuergeheimnis etc.)
Grundschutz	INTERN	Schutzniveau 1	Allgemeine Personendaten
	Nicht klassifiziert	Schutzniveau 0	Nicht personenbezogene Daten (ausserhalb des Schutzbereichs des KDSG)
Personensicherheitsprüfung nach ICSG durch anstellende Behörde		Vollzugsvorschriften für ICSG und KDSG	Prüfung der Vertrauenswürdigkeit nach Personalgesetz durch anstellende Behörde