

Dezember 3/2025

Neues Fallführungssystem für die Sozialdienste, die Kindes- und Erwachsenenschutzbehörden und die Arbeitsintegration (NFFS)

Verordnung über die Informations- und Datensicherheit IDSV
E-Government? - Aber sicher!

KPG-Finanzbulletin

Erscheint viermal jährlich und ist das offizielle Organ für die Mitglieder der KPG Bern

Redaktionsteam

Monika Gerber, BGK
Daniela Jaussi, KPG
Iris Markwalder, AGR

Redaktionsadresse

KPG Bern – GAC Berne
Schwarztorstrasse 20, 3007 Bern
Telefon 031 385 20 00
gemeindefinanzen@kpgbern.ch
www.kpgbern.ch

Inhaltsverzeichnis

Seite

Editorial

Daniela Jaussi

1 - 2

Fachbeiträge

3 - 13

Fallführungssystem

Manuel Michel, Vorsteher Amt
für Integration und Soziales
des Kantons Bern

3 - 6

Verordnung über die Informations-
und Datensicherheit IDSV

Sascha Tarli, stv. Leiter Recht
Amt für Informatik und Organi-
sation des Kantons Bern

7 - 13



Editorial

Daniela Jaussi, Leiterin Bereich Gemeindefinanzen, KPG Bern

Liebe Leserin, lieber Leser

Mit einer kleinen Verspätung halten Sie das Finanzbulletin des letzten Dezembers in Ihren Händen.

Im ersten Beitrag erläutert Ihnen Manuel Michel, Vorsteher des Amtes für Integration und Soziales des Kantons Bern, fundiert das neue Fallführungssystem für die Sozialdienste, die Kindes- und Erwachsenenschutzbehörden und die Arbeitsintegration, abgekürzt NFFS genannt. Er erklärt die Vorteile des neuen Systems, verschweigt nicht, dass es bei der Einführung durch die Gemeinden einen personellen und auch finanziellen Effort braucht und dass noch gewisse Herausforderungen bestehen, bis die Einführung erfolgreich abgeschlossen werden kann.

Der zweite Beitrag stammt von Sascha Tarli, stv. Leiter Recht beim Amt für Informatik und Organisation des Kantons Bern. Er bringt uns das Thema E-Government näher und führt aus, weshalb damit Fragen zu Daten- und Informationssicherheit so wichtig werden. Für die Gemeinden (Einwohner-, Kirch- und Burgergemeinden) bedeutet das, dass sie sorgfältig mit Daten umgehen und sie auch vor unrechtmässiger Verwendung, also Datendiebstahl oder Cyberangriffen, schützen müssen.

Beide Beiträge dürfen gerne auch an weitere Personen geschickt werden, es handelt sich meiner Meinung nach um Themen, die einen grösseren Kreis von Gemeindefachleuten interessieren dürften.

Ich habe von Monika Gerber, sie ist im Redaktionsteam des Finanzbulletins, betreut die Geschäftsstelle des BGK und ist stellvertretende Geschäftsführerin des VBG, den Hinweis erhalten, dass die Steuerverwaltung per 1. Januar 2025 ihre Praxis bei den Entschädigungen für reine Milztätigkeit in Gemeindebehörden und -kommissionen angepasst hat. [Hier](#) finden Sie die entsprechenden Ausführungen der kantonalen Steuerverwaltung zur steuerlichen Behandlung bzw. zur Deklaration im Lohnausweis.

Und zu guter Letzt möchte ich Sie über eine Änderung bei der KPG informieren: unser Geschäftsführer, Adrian Mauerhofer, hat sich auf Ende 2025 pensionieren lassen. Seine Nachfolge übernimmt Maya Hofer. Für weitere Informationen zu unserer neuen Geschäftsführerin verweise ich gerne auf unsere Homepage www.kpgbern.ch/de/aktuell.

Ich wünsche Ihnen eine spannende Lektüre und ein gutes, erfolgreiches 2026!

Daniela Jaussi





Verordnung über die Informations- und Datensicherheit IDSV

*Sascha Tarli, stv. Leiter Recht Amt für Informatik und Organisation des Kantons Bern
Fürsprecher / Executive MPA unibe / CAS Information Security hslu
Ehem. Gemeinderat von Vechigen*

E-Government? - Aber sicher!

Seit dem 1. März 2023 gilt für die Behörden im Kanton Bern die Pflicht zur digitalen Verwaltungsführung. Diese bringt der Bevölkerung und Wirtschaft viele Vorteile, birgt aber auch Risiken für Informationen und Personendaten. Deren Sicherheit ist entscheidend für das Vertrauen in den Staat. Dafür sollen das Gesetz über die Informations- und Cybersicherheit (ICSG), das neue Datenschutzgesetz (KDSG) und deren Ausführungsverordnung IDSV sorgen, welche in die Konsultation gegeben wurde.

Die digitale Verwaltungsführung (E-Government) hat im Kanton Bern bis heute schon zu einigen praktischen und sehr nutzerfreundlichen Applikationen geführt, z.B. TaxMe, E-Umzug, E-Bau, E-Payment, E-Police, Kibon (Betreuungsgutscheine), Stipendien Online, GRUDIS Public (Grundbuch) oder Subene (Förderprogramm Energie).¹ Dazu werden weitere Applikationen auch des Bundes kommen, wie E-Collecting (Sammeln von Unterschriften für Referenden oder Initiativen), E-Voting und insbesondere auch die E-ID, welche die Zugänglichkeit und Sicherheit von E-Gov-Applikationen künftig stark erhöhen wird.

Gerade die letzten Beispiele zeigen, wie wichtig die Informations- und Datensicherheit für das Vertrauen der Bevölkerung in den Staat ist. Nicht auszudenken wären die Folgen für die Schweiz, wenn deren Abstimmungen oder Wahlen von feindlichen Mächten via Hacking gefälscht würden.

Aber auch schon die Vorstellung, dass die finanziellen Verhältnisse von Familien im so genannten Darknet² auftauchen, hinterlässt ein schlechtes Gefühl.

¹ Eine Übersicht über die E-Services BE findet sich auf dem [Internetportal des Kantons Bern](#).

² Das Darknet ist ein verborgener, verschlüsselter Teil des Internets, der nicht über normale Suchmaschinen wie Google erreichbar ist und spezielle Software wie den Tor-Browser benötigt, um darauf zuzugreifen. Es bietet Anonymität und ist sowohl für legitime Zwecke wie Zensurumgehung durch Journalisten und Aktivistinnen als auch für illegale Aktivitäten wie den Handel mit Drogen und Waffen durch Kriminelle bekannt.

Die Bevölkerung vertraut der digitalen Welt nur, wenn sie sich darin sicher fühlt. Die Strategie «Digitale Schweiz 2026»³ des Bundesrates, gültig ab dem 1. Januar 2026, führt daher «Sicherheit und Vertrauen» sogar als eigenen Wirkungsbereich mit eigenen Messgrössen auf: «Die Einwohnerinnen und Einwohner der Schweiz können sich in der digitalen Welt sicher bewegen; die Privatsphäre ist geschützt.»⁴.

Jede zweite Gemeinde unsicher

Europa und die Schweiz müssen sich besser, insbesondere auf russische Cyberattacken, vorbereiten. Dieser Appell stammt vom Bundesamt für Cybersicherheit (BACS) anlässlich des Ukraine-Gipfels auf dem Bürgenstock vom Mai 2024.⁵ Leider bestätigte sich diese Warnung durch den Angriff vom Januar 2025 der pro-russischen Hackergruppe NoName auf den Kanton Schaffhausen, die Städte Genf und Siders und auf mehrere Luzerner Gemeinden.⁶ NoName hatte bereits im Juni 2023 das Schweizer Parlament angegriffen.⁷ Der Bundesrat formuliert denn auch im Entwurf zu seiner sicherheitspolitischen Strategie der Schweiz 2026⁸ die Massnahme 8 wie folgt: «Die Cybersicherheit *aller Staatsebenen*, der Unternehmen, der Wissenschaft und der Gesellschaft wird *umfassend* verbessert.».

Es ist also für alle unbestreitbar ersichtlich: Die Schweiz, die Kantone und die Gemeinden müssen besser gegen Cyberangriffe gerüstet sein.

Der Schweizerische Gemeindeverband stellte im Juni 2025 aber fest, dass jede zweite Gemeinde ungenügend auf Cyberangriffe vorbereitet ist.⁹ Dies musste bereits im November 2023 auch die Gemeinde Zollikofen erfahren: Die Gemeindeverwaltung wurde gehackt, so dass weder Computer noch Telefone funktionierten.¹⁰ Die Gemeinde hat unterdessen in die Informations- und Datensicherheit investiert und lässt ihre ICT-Mittel zudem regelmässig auf Schwachstellen überprüfen.

³ Bundesrat, Strategie «Digitale Schweiz 2026», vom 12. Dezember 2025

⁴ Strategie Digitale Schweiz 2026, Wirkungsbereich «Sicherheit und Vertrauen»

⁵ Artikel SRF vom 31. Mai 2025

⁶ Artikel Swissinfo vom 22. Januar 2025

⁷ Artikel SRF vom 16. Juli 2025

⁸ Entwurf vom 12. Dezember 2026 zur sicherheitspolitischen Strategie der Schweiz 2026 z.H. Vernehmlassung

⁹ Publikation Schweizerischer Gemeindeverband vom 18. Juni 2025

¹⁰ Artikel SRF vom 19. Juni 2025

Und die Stadt Bern gab im Februar 2024 bekannt, dass sie im Vorjahr 23 Millionen Cyberangriffe verzeichnete.¹¹ Die Sicherheit müsse deshalb ständig weiterentwickelt werden, wie der damalige Stadtpräsident betonte.

IDSV: Doppelte Sicherheit

Im Kanton Bern bestehen u.a. die folgenden gemeinderechtlichen Körperschaften (Stand September 2025):

- 233 Kirchgemeinden,
- 335 Einwohnergemeinden, und
- 250 Burgergemeinden oder burgerliche Korporationen

Diese rund 800 Gemeindebehörden weisen einen sehr unterschiedlichen Reifegrad der Informations- und Datensicherheit auf. Die Pflicht zur Informations- und Datensicherheit betrifft die Stadt Bern ebenso wie die kleinste Berner Einwohnergemeinde Schelten mit ihren 34 Einwohnerinnen und Einwohnern, die katholische Kirchgemeinde Adelboden oder die Bergbäuert Reichenbach.

Nicht nur wegen der grossen Unterschiede der Grösse und Ressourcen haben die gemeinderechtlichen Körperschaften teilweise Mühe, die Informations- und Datensicherheit zu gewährleisten. Sondern auch die Tatsache, dass die Informations- und Datensicherheit eine recht technische und damit abstrakte Materie ist, verlangt besondere Anstrengungen. Zudem fehlen im Kanton Bern bis anhin klare und verbindliche Regeln, bei deren Befolgung die Berner Behörden wissen, dass sie ihre Pflichten zur Informations- und Datensicherheit erfüllen.

Auch vor diesem Hintergrund hat der Bund mit dem Erlass seines Informationssicherheitsgesetzes (ISG)¹² sowie der Verordnung über die Cybersicherheit (CSV)¹³ die Betreiberinnen kritischer Infrastrukturen dazu verpflichtet, zum Schutz potenziell weiterer Opfer innert 24 Stunden nach Entdeckung einen Cyberangriff zu melden.

¹¹ [Artikel Der Bund vom 7. Februar 2024](#)

¹² ISG, [SR 128](#)

¹³ CSV, [SR 128.51](#)

Diese Pflicht betrifft ausnahmslos alle oben aufgezählten gemeinderechtlichen Körperschaften, auch wenn sie kein Rechenzentrum oder Stromwerk betreiben, das ISG und die CSV machen hier keine Ausnahmen.¹⁴ Bei Verletzung der Meldepflicht droht seit dem 1. Oktober 2025 den Verpflichteten eine Busse von bis zu CHF 100'000.¹⁵

Doch: Was ist eine meldepflichtige Schwachstelle oder ein meldepflichtiger Cyberangriff? Und nach welchen Regeln und auf welchem Weg sind diese zu melden? Und überhaupt: Wann sind die Informationen und Personendaten sicher genug?

Die Grundregeln hierfür finden sich in zwei neuen Gesetzen des Kantons Bern:

- a) Das Gesetz über die Informations- und Cybersicherheit (ICSG)¹⁶, vom Grossen Rat am 12. Juni 2025 einstimmig beschlossen; Ablauf der ungenutzten Referendumsfrist am 2. Oktober 2025.
- b) Das totalrevidierte Datenschutzgesetz (KDSG)¹⁷, welches am 3. Dezember 2025 in zweiter Lesung vom Grossen Rat beschlossen wurde.

Beide Gesetze sollen Mitte 2026 in Kraft treten. Sie regeln im Grundsatz und generell-abstrakt die Informations- und Datensicherheit.

Konkretere Antworten wird die IDSV liefern. Sie gibt den Berner Behörden verbindliche, generell-konkrete organisatorische, technische, physische und personelle Massnahmen vor für die Gewährleistung der rechtmässigen Informations- und Datensicherheit. Wer diese Massnahmen risikoorientiert umsetzt, hat doppelte Sicherheit: Sicherheit für die Informationen und Personendaten sowie Sicherheit der rechtmässigen Verwaltungsführung.

IDSV: Auch auf Gemeinden zugeschnitten

Ein wichtiges Ziel der IDSV ist der *risikoorientierte* Schutz von Informationen und Personendaten, der wie folgt auf den Punkt gebracht werden kann: Holz auf die Scheiterbeige, Gold in den Safe!

¹⁴ [Art. 74b Abs. 1 Bst. b ISG, Meldepflichtige Gemeindebehörden](#), i.V.m. [Art. 12 CSV, Ausnahmen von der Meldepflicht](#)

¹⁵ [Art. 74g](#) und [Art. 74h ISG](#)

¹⁶ ICSG, [Referendumsfassung](#)

¹⁷ KDSG, [Referendumsfassung](#)

Dies erfolgt in drei Schritten:

1. Der wichtigste erste Schritt ist also das Holz vom Gold zu trennen. Welche Informationen müssen vertraulich oder gar geheim bleiben? Welche Personendaten sind besonders zu schützen? Die sog. Schutzobjekte sind nach ihrer Bedeutung zu inventarisieren.
2. In einem zweiten Schritt sind die aktuellen und künftigen Fähigkeiten der «Panzerknacker» zu bestimmen, also die Grösse der Risiken pro Schutzobjekt zu beschreiben.
3. Im dritten Schritt wird aus der Bedeutung der Schutzobjekte und der Grösse der Risiken die «Stärke der Safe-Wand» festgelegt; also werden die erforderlichen Schutzmassnahmen pro Schutzobjekt bestimmt.

Dies soll zum Ergebnis führen, dass künftig *weniger Schutzobjekte vorliegen, diese aber besser geschützt* sind. Dies spart den Behörden Arbeit und damit Kosten und soll auch ihre Arbeit vereinfachen. Die Gemeinden aber arbeiten fast nie mit geheimen Informationen, im Gegensatz zu den kantonalen Behörden, z.B. bei der verdeckten Ermittlung gegen das organisierte Verbrechen.

Beim risikoorientierten Schutz ist auch die Anzahl der Schutzobjekte wichtig; sie bestimmt das Ausmass des Schadens beim Eintritt von Risiken mit. So sind im kantonalen Bevölkerungsregister rund eine Million meldepflichtige Personen gespeichert, im Einwohnerregister der Gemeinde Schelten jedoch nur 34. Daher unterscheidet die IDSV zwischen Regeln für die Kantonsverwaltung und Regeln für die Gemeinden. Von den 45 Artikeln der IDSV formulieren nur 18 Artikel Pflichten und Aufgaben für die Einwohner-, Kirch- und Burgergemeinden.

IDSV: Praxisorientiert und wirkungsstark

Die Vorschriften der IDSV müssen für die betroffenen Organisationen mit verhältnismässigem Aufwand umsetzbar, effektiv und effizient sein. Zu diesem Zweck wurde der Entwurf zur IDSV unter Einbezug der folgenden Behörden und Unternehmen erarbeitet:

- Das Staatssekretariat für Sicherheitspolitik des Bundes (SEPOS) und das Bundesamt für Cybersicherheit (BACS)
- Die Datenschutzaufsichtsstelle des Kantons Bern

- Die Bau- und Verkehrsdirektion, die Direktion für Inneres und Justiz sowie die Sicherheitsdirektion des Kantons Bern
- Die Stadt Bern sowie die Einwohnergemeinden Lyss und Grossaffoltern
- Der Verband Bernischer Gemeinden (VBG), der Verband bernischer Burgergemeinden und burgerlicher Korporationen (VBBG) sowie der Kirchgemeindeverband des Kantons Bern (KVG)
- Pädagogische Hochschule, Universität Bern und Berner Fachhochschule
- Swisscom AG, SPIE Schweiz AG sowie Bedag Informatik AG

Zudem wurden die beiden ICT-Unternehmen Talus AG und Dialog Verwaltungs-Data AG zum Mitberichts- und Konsultationsverfahren eingeladen, beides ICT-Unternehmen, welche zusammen die grosse Mehrheit der Berner Einwohnerkontrollen als Kunden haben. Also nicht nur die verantwortlichen Behörden jeder Staatsebene, sondern auch die potenziell mit ICT-Leistungen beauftragten Unternehmen sollen gewährleisten, dass die IDSV nur umsetzbare und wirkungsvolle Massnahmen für den so genannten Grundschutz vorschreibt.

Am 8. Dezember 2025 wurde das Mitberichts- und Konsultationsverfahren gestartet, bis am 30. Januar 2026 werden die Stellungnahmen erwartet.

Unterstützung der Gemeinden

An dieser Stelle machen wir gerne auf die bereits heute vorhandenen Hilfsmittel des kantonalen Amtes für Informatik und Organisation (KAIO) für die Informations- und Datensicherheit auch für die Gemeinden aufmerksam:

- Das KAIO verfügt über Rahmenverträge, woraus die Behörden zu günstigen Konditionen bei qualifizierten Informations- und Datensicherheitsunternehmen Dienstleistungen auf eigene Kosten abrufen können. Informationen dazu finden sich auf der [Internetseite der Zentralen Beschaffungsstelle ICT des KAIO](#).
- Das KAIO schult die Mitarbeitenden der Kantonsverwaltung in der Informations- und Datensicherheit via dem Web-Based-Training (WBT) [BE-Secure](#). Dieses ist öffentlich zugänglich und kann von Mitarbeitenden von Gemeinden, Lehrpersonen, Schülerinnen und Schülern und vielen weiteren Personen bearbeitet werden.

- Der Kanton Bern erliess für die kantonalen Behörden per 1. Januar 2025 die [Weisung über den Grundsatz für die Informations- und Cybersicherheit \(ICSGW\)](#). Sie enthält im Anhang 4 die [Allgemeinen Geschäftsbedingungen des Kantons Bern über die Informationssicherheit und den Datenschutz \(AGB ISDS BE\)](#). Deren Einsatz zusammen mit den kantonalen [Vorlagen zu den ICT-Verträgen für die Beauftragung Dritter](#) gewährleisten einen guten Grundsatz.
- Die Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) stellt den kantonalen und kommunalen Verwaltungen ein [E-Learning-Portal zur Informationssicherheit für Behörden](#) zur Verfügung. Insgesamt sind auf dem Portal dreizehn Module verfügbar, ein Modul ist noch in Vorbereitung.

Mit der IDSV verfügen insbesondere auch die Gemeinden künftig über ein stark verbessertes Rüstzeug für ihre sichere und damit vertrauenswürdige elektronische Verwaltungsführung im Dienste der Bevölkerung.