Kanton Bern
Canton de Berne

Jahresbericht Datenschutzaufsichtsstelle 2025

Impressum

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

Layout und Realisation: noord.ch
Illustrationen: aurelmaerki.ch

1 Vorwort

«Jetzt haben Sie mir die Angst genommen!» Diese Rückmeldung nach einem Austausch mit Gemeindeschreiberinnen und Gemeindeschreibern über das neue Datenschutzgesetz freute mich sehr. Der Datenschutz soll niemandem Angst machen! Die wichtigsten Regeln, die bereits in unserer Kantonsverfassung stehen und nicht geändert werden, sind nämlich gar nicht so kompliziert – wenn man sie verständlich erklärt: So bedeutet das «Gesetzmässigkeitsprinzip», dass eine Gemeindeangestellte Personendaten bearbeiten darf, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben nötig ist. Kann sie nachvollziehbar erklären, warum sie die Daten für ihre Arbeit braucht, ist die Bearbeitung auch erlaubt. Und das «Verhältnismässigkeitsprinzip» heisst nichts anderes, als dass nur diejenigen Daten bearbeitet werden sollen, die wirklich erforderlich (und nicht nur praktisch) sind, und dass sie nur so lange aufbewahrt werden wie nötig.

Auch die betroffenen Personen verstehen ihre Rechte und deren Grenzen viel besser, wenn man sie ihnen anhand konkreter Beispiele erklärt – etwa, warum ihnen keine zentrale Stelle Auskunft darüber geben kann, welche Daten in der gesamten Verwaltung über sie bearbeitet werden (siehe auf der DSA-Website unter «Aktuelles» den Beitrag vom 4. November 2025).

Im Rahmen ihres Beratungsauftrags gegenüber Behörden und Betroffenen achtet die DSA daher vermehrt darauf, ihr Informationsangebot zur Sensibilisierung und Aufklärung auf das breite Publikum auszurichten und für dieses interessant und verständlich zu machen. Wer sich der Kernanliegen des Datenschutzes bewusst geworden ist und die (wenigen!) rechtlichen Grundsätze als solche verstanden hat, wird allein mit seinem gesunden Menschenverstand schon sehr viel richtig machen.

Anders verhält es sich mit der Informationssicherheit. In einer digitalen und vernetzten Welt, in der weder die zu schützenden Daten noch die Risiken bzw. die Angreifer, von denen diese ausgehen, sicht- und greifbar sind, hilft blosse Intuition nicht mehr weiter. Hier muss ein strukturiertes Vorgehen Klarheit schaffen, damit die richtigen Massnahmen getroffen werden können. Es wird deshalb ein besonderes Anliegen der DSA sein, den Gemeinden die Risiken bei der Digitalisierung ihrer Datenbearbeitungen sowie Wege aufzuzeigen, wie sie diese auf ein tragbares Mass bringen können. Dabei geht es nicht nur um die Vertraulichkeit der Daten, sondern insbesondere auch um deren Verfügbarkeit. Hat nämlich eine Gemeinde plötzlich keinen Zugriff mehr auf ihre Daten, so kann sie selbst ihre grundlegendsten Aufgaben nicht mehr ordnungsgemäss oder gar nicht mehr erfüllen.

Datenschutz liegt also nicht nur im Interesse der Bürgerinnen und Bürger, sondern auch der Gemeindebehörden selbst. Entsprechend braucht es zweierlei: ansprechende Informationen für alle und professionelle Beratung für Behörden. In diesem Sinne freuen wir uns auf das Inkrafttreten des neuen Datenschutzgesetzes und auf eine angstfreie Zusammenarbeit mit den Gemeinden.

Ueli Buri, Datenschutzbeauftragter

2 Das Fundament unserer Arbeit

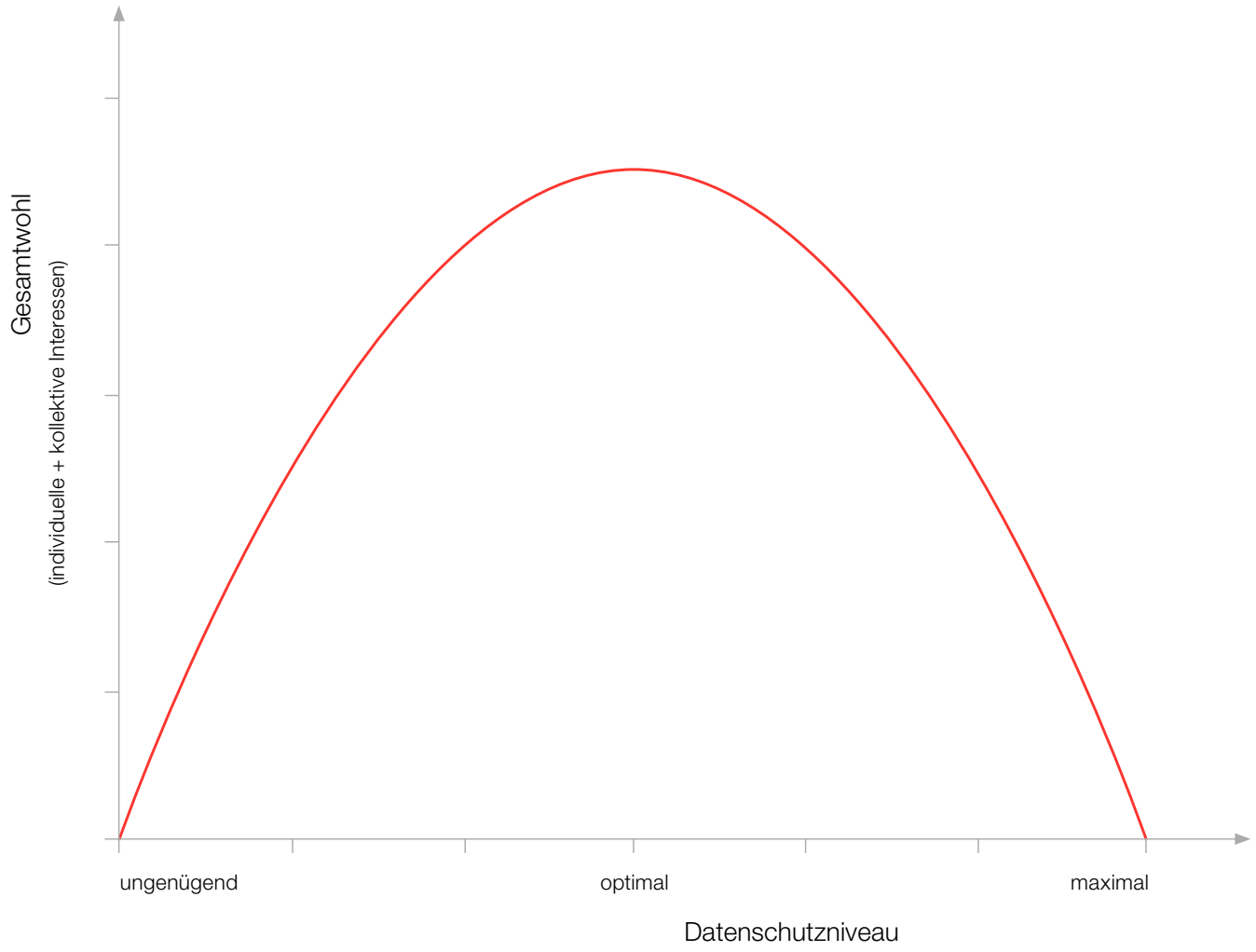
Grundrecht auf Datenschutz

Datenschutz ist kein Nice-to-have, sondern ein Grundrecht – diese Worte fielen im Grossen Rat, als das revidierte Datenschutzgesetz in erster Lesung verabschiedet wurde. Und sie bringen es auf den Punkt: Der Schutz der Privatsphäre einschliesslich des Rechts auf informationelle Selbstbestimmung (d. h. des Rechts jeder Person, darüber bestimmen zu können, ob und zu welchem Zweck Daten über sie bearbeitet werden) ist ein von der Bundes- und der Kantonsverfassung geschütztes Grundrecht. Jede Einschränkung von Grundrechten – also auch die Bearbeitung von Personendaten durch Behörden – ist nur unter bestimmten Voraussetzungen zulässig. Sie muss sich auf eine hinreichende gesetzliche Grundlage stützen, einem überwiegenden öffentlichen Interesse dienen und mit Blick auf ihren Zweck verhältnismässig sein (sprich: *geeignet, notwendig* und für die betroffenen Personen *zumutbar*). Zum Grundrecht auf Datenschutz gehört gemäss Berner Verfassung auch, dass die bearbeiteten Daten korrekt sein müssen und vor missbräuchlicher Verwendung zu schützen sind (Datensicherheit).

Wenn ein individuelles Grundrecht auf kollektive Interessen trifft

Oben ist es bereits angedeutet: Kein Grundrecht gilt absolut und ohne Ausnahme. Dieselbe Verfassung, die das Recht auf Privatsphäre garantiert, weist den kantonalen und kommunalen Behörden Aufgaben zu, die sie im Interesse der Gemeinschaft erfüllen müssen – etwa in den Bereichen Bildung, Gesundheit, Wirtschaft oder Sicherheit. Zu diesem Zweck müssen Behörden auch Personendaten bearbeiten können. Damit stehen sich zwei Interessen gegenüber: das individuelle Recht auf Privatsphäre und der kollektive Anspruch auf ein funktionierendes Gemeinwesen.

Den von der Verfassung gewährleisteten Datenschutz verstehen wir deshalb als *angemessenen* Datenschutz, der diese beiden Interessen zum bestmöglichen Ausgleich bringt. Das optimale Schutzniveau liegt beim höchsten Gesamtwohl aus der Verwirklichung individueller und kollektiver Interessen. Zur Veranschaulichung dient folgende Kurve:



Nicht zu wenig, nicht zu viel

Ist der Datenschutz zu schwach, werden individuelle Grundrechte verletzt. Ist er zu streng, können Behörden ihre Aufgaben nicht mehr erfüllen – was wiederum das Recht der Bürgerinnen und Bürger auf ein funktionierendes Gemeinwesen beschneidet.

Von Rechten und Pflichten: das KDSG

Das kantonale Datenschutzgesetz (KDSG) – sowohl das bestehende als auch das revidierte – konkretisiert die *Pflichten der Behörden* beim Bearbeiten von Personendaten. Nebst der Verwaltung gelten auch andere Träger öffentlicher Aufgaben (wie etwa Schulen und Spitäler) als Behörden. «Bearbeiten» meint jedweden Umgang mit Personendaten: vom Beschaffen über das Aufbewahren, Verändern, Verknüpfen und Bekanntgeben bis hin zum Vernichten. Daten dürfen nur zu einem bestimmten Zweck beschafft und grundsätzlich nicht für andere Zwecke bearbeitet werden.

Auch die *Rechte der Betroffenen* werden im KDSG geregelt, namentlich das Recht auf Auskunft und Einsicht in ihre Daten, auf Berichtigung falscher und auf Löschung nicht benötigter Angaben über sie.
Darüber, dass die Behörden ihre Pflichten im Einklang mit den Rechten der Betroffenen erfüllen, wachen die kantonalen und kommunalen Datenschutzaufsichtsstellen. Ihre Stellung und Aufgaben sind ebenfalls im KDSG festgehalten.

An diesen Grundsätzen ändert die im Dezember verabschiedete Gesetzesrevision nichts. Sie schliesst bestehende Lücken, konkretisiert und verbessert den Datenschutz und gibt der DSA mehr aufsichtsrechtliche Mittel an die Hand. Die für uns zentrale Änderung ist die Ausdehnung unseres Zuständigkeitsbereichs. Künftig stehen wir 330 politischen Gemeinden und über 700 kommunalen Körperschaften als Beratungs- und Aufsichtsstelle zur Seite – eine Herausforderung für uns, aber auch eine grosse Chance für die Professionalisierung des Datenschutzes auf allen Ebenen.

3 Verantwortung und Aufsicht

Die Verantwortung für Datenschutz und Informationssicherheit liegt bei den Behörden selbst. Jede Institution, die zur Erfüllung ihrer gesetzlichen Aufgaben Daten bearbeitet oder durch Dritte bearbeiten lässt, muss für die Einhaltung der Vorschriften sorgen. Das gilt für alle Datenbearbeitungen und unabhängig davon, ob diese von der zuständigen Aufsichtsstelle geprüft worden sind oder nicht.

Datenschutz auf drei Ebenen

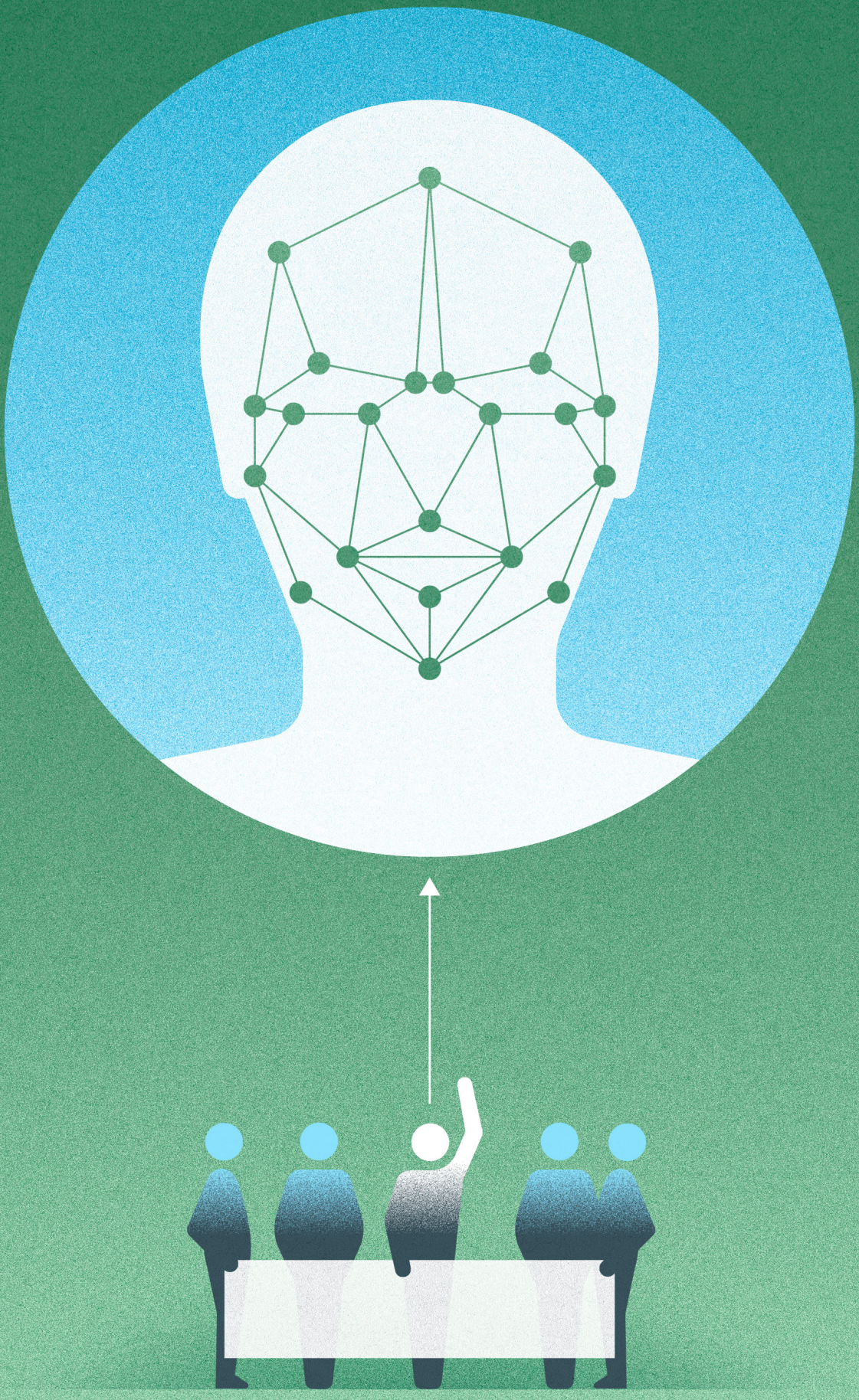
Das Datenschutzrecht ist hierzulande föderalistisch aufgebaut: Für *Bundesbehörden und Private* gilt das Datenschutzgesetz des Bundes (DSG) und die Aufsicht obliegt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Wenn also ein Detailhändler seine Einstellhalle videoüberwachen möchte, muss er sich an den EDÖB wenden – auch dann, wenn die betroffene Filiale in Boltigen, Belprahon oder Bern steht.

Für kantonale und kommunale Behörden im Kanton Bern gilt das KDSG. Die Aufsicht ist hier bislang zweigeteilt: Die DSA ist für *kantonale Behörden* zuständig, während *Gemeinden und andere kommunale Körperschaften* je eigene Aufsichtsstellen haben. Über Letztere übt die DSA die Oberaufsicht aus. Mit Inkrafttreten des revidierten KDSG (vermutlich ab September 2026) wird diese Zweiteilung für die meisten Gemeinden aufgehoben und die Datenschutzaufsicht zentralisiert.

Mehrere Ebenen im selben Unternehmen: Beispiel Inselspital

Nicht immer ist die Trennung der Ebenen so klar wie oben beschrieben. Kompliziert wird es zuweilen, wenn ein Privatunternehmen öffentliche Aufgaben übernimmt. Ein Beispiel dafür ist das Inselspital. Als Teil der Insel Gruppe AG untersteht es zunächst den Vorschriften des DSG für private Datenbearbeiter und der Aufsicht des EDÖB. Für die Daten des Spitalpersonals oder die Videoüberwachung eines reinen Personalparkplatzes ist die DSA deshalb nicht zuständig. Soweit das Inselspital aber Leistungen der medizinischen Grundversorgung erbringt, handelt es im Auftrag des Regierungsrats und gilt damit als Behörde im Sinne des KDSG. Zuständig ist in diesen Fällen die DSA. Bei sogenannten überobligatorischen Leistungen – etwa im Bereich der Schönheitschirurgie – handelt das Spital wiederum als Privatunternehmen nach den Regeln des DSG und unter der Aufsicht des EDÖB.

Bei der Bearbeitung von Patientendaten entscheiden also Art und Anlass der medizinischen Behandlung darüber, wer die Datenschutzaufsicht ausübt. Für die Videoüberwachung im Insel-Parking bedeutet das: DSA und EDÖB teilen sich die Zuständigkeit – schliesslich verkehren dort Patientinnen und Besucher jeder Kategorie. Die DSA verlangt für solche Videoüberwachungen Vorabkontrollen und führt Audits durch, weil die Anforderungen aus dem Grundrechtsschutz strenger sind als im Privatrecht.



4 Unser Selbstverständnis: vorbeugen statt eskalieren

Die gesetzlichen Aufgaben der DSA sind in Artikel 34 KDSG aufgelistet. Wir verstehen unseren Auftrag wie folgt: Die DSA unterstützt die kantonalen Behörden bei der Wahrnehmung ihrer Verantwortung für den Datenschutz und die Datensicherheit. Sie berät die Behörden informell und nimmt formell Stellung zu Erlassentwürfen und anderen datenschutzrelevanten Massnahmen sowie zu geplanten elektronischen Datenbearbeitungen mit besonderen Risiken für die Betroffenen (Vorabkontrollen). Zudem führt sie Informationssicherheitsprüfungen bei bereits in Betrieb stehenden Systemen und Applikationen durch (Audits). Betroffenen Personen steht die DSA als Anlaufstelle für Beratung, Vermittlung und für die Behandlung von Beschwerden zur Verfügung. Erweist es sich zur Durchsetzung eines angemessenen Datenschutzes als unvermeidbar, so kann die DSA gegenüber Behörden begründete Anträge stellen und ablehnende Verfügungen mit Beschwerde bis vor das Verwaltungsgericht bringen. Dies soll aber nur als Ultima Ratio geschehen, wenn die lösungsorientierte Beratung und Zusammenarbeit nicht zum Erfolg führen. Im Vordergrund unserer Arbeit steht die präventive Aufsicht, die den Behörden frühzeitig die Spielräume aufzeigt und entsprechend besser akzeptiert wird. Mit dem Register über die von kantonalen Behörden geführten Datensammlungen stellen wir Transparenz her, damit Betroffene ihre Rechte auf Auskunft und Einsicht (sowie ggf. Berichtigung oder Löschung) wahrnehmen können.

5 Unsere Ressourcen

5.1 Das Team

Per 31. Dezember 2025 verfügte die DSA über einen Personalbestand von 750 Prozent, aufgeteilt auf neun Personen. Vier davon sind juristisch ausgebildet, vier sind Informatiker bzw. Informatikprüfer und eine ist Journalistin/Redaktorin:

Ueli Buri (Datenschutzbeauftragter) ist Rechtsanwalt und leitet die DSA seit 2019. Er verantwortet die Festlegung der strategischen Ausrichtung und jährlichen Leistungsziele der DSA sowie deren personelle und betriebliche Führung. Fachlich betreut er primär drei Direktionen – Bau und Verkehr, Inneres und Justiz (DIJ) und Sicherheit –, die Staatskanzlei (STA) sowie die Justizbehörden.

Anders Bennet (stellvertretender Datenschutzbeauftragter Informatik) ist Informatiker und war über zehn Jahre für den Kanton Bern in der Rolle als interner Informatik-Revisor tätig. Teil des DSA-Teams war er von 2019 bis zum 31. Dezember 2025. Seine Hauptaufgabe bestand darin, bereits laufende IT-Systeme und Anwendungen zu prüfen (d. h. Audits zu planen und durchzuführen) sowie die Umsetzung organisatorischer und technischer Massnahmen im Bereich Informationssicherheit und Datenschutz (ISDS) zu begleiten.

Rahel Lutz (stellvertretende Datenschutzbeauftragte Recht) ist Rechtsanwältin und arbeitet seit 2009 bei der DSA. Sie betreut die Gesundheits-, Sozial- und Integrationsdirektion (GSI) sowie zahlreiche Spitäler und andere Gesundheitseinrichtungen in datenschutzrechtlichen Fragen bei der Gesetzgebung und der Erfüllung gesetzlicher Aufgaben. In Vorabkontrollen prüft sie die eingereichten ISDS-Dokumente im Hinblick auf rechtliche Aspekte.

Christina Hug Gnägi (wissenschaftliche Mitarbeiterin Recht) ist Rechtsanwältin und arbeitet seit April 2024 bei der DSA. Sie betreut hauptsächlich Beratungs-, Gesetzgebungs- und Vorabkontrollgeschäfte im Aufgabenbereich der GSI (Verwaltung und Gesundheitseinrichtungen) sowie der Wirtschafts-, Energie- und Umweltdirektion (WEU). Zudem berät und beaufsichtigt sie die kantonalen Behörden bei geplanten Videoüberwachungen.

Bianca Hüsing (Kommunikationsleiterin) hat nach dem Studium der Germanistik und der Philosophie eine journalistische Laufbahn absolviert und verfügt über langjährige Erfahrung als Redaktorin einer bernischen Regionalzeitung. Seit August 2025 sorgt sie dafür, dass die DSA den gesetzlichen Beratungs- und Informationsauftrag gegenüber den Behörden und der Öffentlichkeit gezielt und in verständlicher Sprache erfüllt.

Samuel Kaufmann (wissenschaftlicher Mitarbeiter Informatik) ist seit 2016 in der IT-Entwicklung und seit 2023 bei der DSA tätig, wo er Behörden zu Fragen der Informationssicherheit berät und technische Vorabkontrollen durchführt.

Jonas Weber (wissenschaftlicher Mitarbeiter Informatik) ist ausgebildeter Spezialist für Informations- und Cybersicherheit und gehört der DSA seit Juli 2025 an. Er berät Behörden in seinem Fachgebiet und führt technische Vorabkontrollen durch.

Michael Weber (wissenschaftlicher Mitarbeiter Recht) ist Rechtsanwalt und gehört der DSA seit 2020 an. Er betreut Auskunfts- und Beratungsgeschäfte, Vorabkontrollen sowie Stellungnahmen zu Erlassen im Bereich der Bildungs- und Kulturdirektion (einschliesslich Berufs-, Mittel- und Hochschulen) sowie der Finanzdirektion (FIN).

Urs Wegmüller (wissenschaftlicher Mitarbeiter Informatik) ist seit dem Jahr 2000 im Bereich der Informationssicherheit tätig und bei der DSA seit 2017 zuständig für die Beratung der Behörden und für technische Vorabkontrollen.

Für die Übernahme der Datenschutzberatung und -aufsicht in den Gemeinden benötigt die DSA vier neue Vollzeitstellen. Davon hat der Grosse Rat in seiner Budgetdebatte mittelfristig nur 3,2 Stellen bewilligt. Er ging davon aus, dass eine Kommunikationsfachperson nur für die Information über die Neuerungen aus der KDSG-Revision benötigt werde, und befristete die Stelle deshalb auf ein Jahr. Dabei übersah er, dass die Beratung 330 politischer Gemeinden und über 700 weiterer gemeinderechtlicher Körperschaften (insbesondere Burger- und Kirchgemeinden sowie Gemeindeverbände) nicht mehr im Verhältnis 1:1 erfolgen kann. Stattdessen wird die DSA vermehrt auf Hilfs- und Informationsangebote setzen müssen, die den – erst noch zu erhebenden – Bedürfnissen der Gemeinden entsprechen. Die Hilfsmittel müssen erstellt und laufend aktuell gehalten werden. Adressatengerechte Kommunikation wird deshalb eine Daueraufgabe der kantonalen Datenschutzbehörde sein.

5.2 Die Finanzen

Im Jahr 2025 wies die DSA einen Aufwand von rund 1,5 Millionen Franken auf, dem ein Ertrag von gut 30.000 Franken gegenüberstand. Nebst den Personalkosten als Hauptposten belief sich der übrige Betriebsaufwand der DSA auf knapp 191.500 Franken. Davon wurden 83,5 Prozent (ca. 160.000 Franken) für externe Dienstleistungen zur Unterstützung von Vorabkontrollen und Informatikprüfungen eingesetzt. Der Ertrag setzt sich zusammen aus Honoraren für externe Weiterbildungen und Entschädigungen für Arbeiten zugunsten von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten.

Die detaillierte Erfolgsrechnung mit Vergleichen zum Budget und zum Vorjahr ist Bestandteil des Geschäftsberichts des Kantons Bern, den die FIN jährlich auf ihrer Website (Themen > Finanzen > Geschäftsbericht) publiziert.

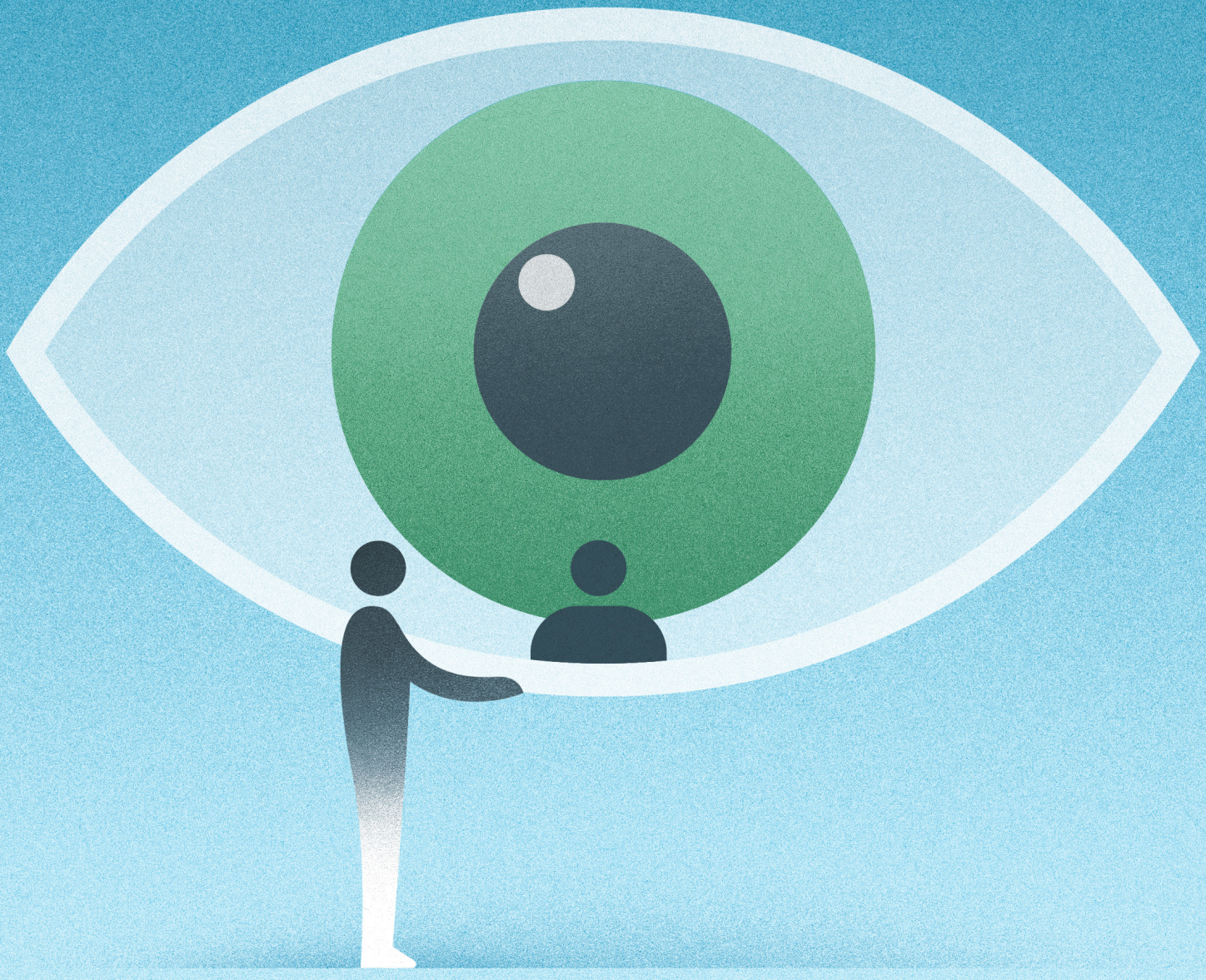
5.3 Das Netzwerk

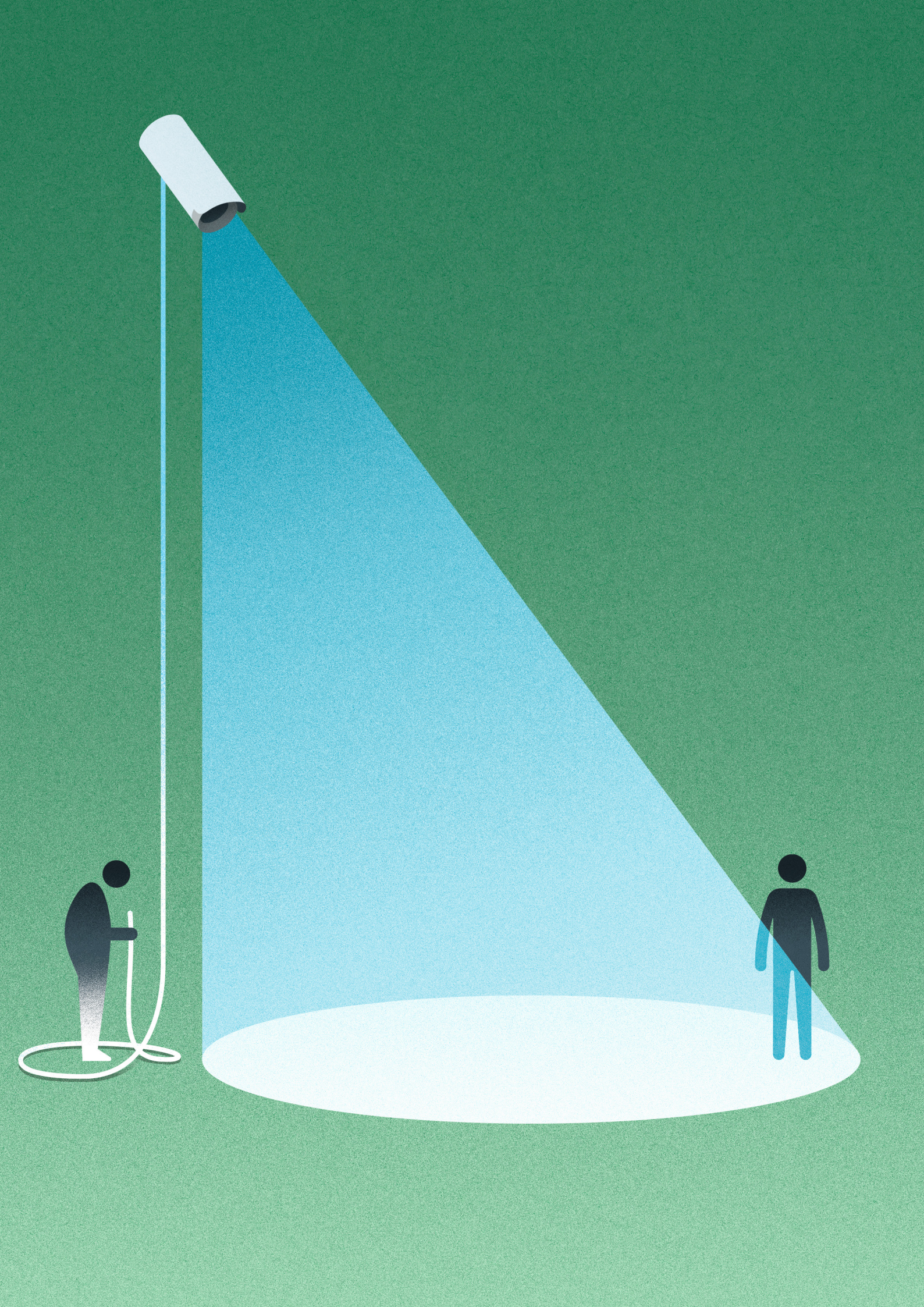
Innerhalb der kantonalen Verwaltung gibt es weitere Anlaufstellen für ISDS-Fragen. So verfügen die Direktionen und die STA je über mindestens eine Kontaktstelle für Datenschutz, die ihre Ämter berät, sowie über eine/n Informationssicherheitsverantwortliche/n (I-SIVE). Gemeindebehörden können sich mit allgemeinen Datenschutzfragen an das Amt für Gemeinden und Raumordnung (AGR) wenden. Für fachspezifische Fragen – etwa zur Digitalisierung der Volksschule – stehen ihnen die Direktionen und die STA zur Verfügung.

Die DSA hat es sich zum Ziel gesetzt, das Bewusstsein und das Wissen betreffend Datenschutz in allen Behörden zu erweitern. Auch in diesem Berichtsjahr führten wir deshalb zwei Anlässe mit allen Datenschutz-Kontaktstellen durch – diesmal zum Schwerpunktthema «Verhältnismässigkeitsprinzip in der Praxis» und zur Totalrevision des KDSG. Mit Blick auf unsere baldige Zuständigkeit für Gemeinden empfingen wir überdies die Aufsichtsstellen der Gemeinden Bern, Biel, Köniz und Thun, die auch unter dem neuen KDSG weiterbestehen werden und mit denen wir uns künftig regelmässig austauschen wollen.

Mit Behörden, denen sich regelmässig anspruchsvolle datenschutzrechtliche Fragen stellen, pflegen wir institutionalisierte Kontakte. Dazu gehören z. B. das Amt für Informatik und Organisation (KAIO), die Bedag Informatik AG, die Kantonspolizei (KAPO), die Insel Gruppe AG sowie weitere Gesundheitseinrichtungen. Im Hinblick auf einen gesamtstaatlich abgestimmten ISDS-Auditplan arbeiten wir ausserdem regelmässig mit der Finanzkontrolle des Kantons zusammen.

Als Mitglied von privatim stehen wir in regelmässigem Kontakt zu den Aufsichtsstellen der anderen Kantone und zum EDÖB. Das Netzwerk dient einerseits dem Wissens- und Erfahrungsaustausch zu Fragen, die sich in allen Kantonen gleichermassen stellen. Andererseits koordinieren die Mitglieder ihre Aufsichtstätigkeit bei Projekten, die über die Kantonsgrenzen hinausreichen (z. B., wenn eine in zahlreichen Kantonen tätige Spitalgruppe ihr Klinikinformationssystem erneuert). DSA-Leiter Ueli Buri ist Mitglied im Büro (Vorstand) und seit November 2020 Präsident von privatim. Rahel Lutz (stellvertretende Datenschutzbeauftragte Recht) leitet die Arbeitsgruppe Gesundheit. In den übrigen fachbezogenen Arbeitsgruppen (zurzeit Digitale Verwaltung, Sicherheit und ICT) wirkt je ein/e Mitarbeiter/in der DSA mit. Welche Themen im Jahr 2025 behandelt wurden, entnehmen Sie dem Bericht unter Ziffer 6.8.





6 Unsere Tätigkeiten: Kostproben aus dem DSA-Alltag 2025

Von der Beratung über die Aufsicht bis hin zur Weiterbildung: Unser Aufgabenspektrum ist breit. Noch vielfältiger sind die Inhalte unserer Arbeit. Mal klären wir für eine Klinik, ob sie die Akten eines Zwangseingewiesenen an dessen Tochter herausgeben darf, mal erläutern wir einer Person im Freiheitsentzug, warum ihre Briefe mitgelesen werden dürfen. An einem Tag nehmen wir Stellung zur kantonalen Gesundheitsplattform, am nächsten Tag beginnt die Vorabkontrolle für eine neue Zivilstands-Software – oder wir prüfen die Serversicherheit eines Spitals gleich vor Ort.

Im Folgenden stellen wir Beispiele aus allen Aufgabenbereichen der DSA vor, die uns 2025 beschäftigt haben und die entweder von besonderer Tragweite oder besonders anschaulich sind.

6.1 Behördenberatung

Sicherer Mailverkehr im Grossen Rat – mühsam, aber unerlässlich

Der Alltag von Grossrätinnen und Grossräten ist anspruchsvoll. Als Privatpersonen, Berufstätige und Volksvertretende füllen sie drei Rollen gleichzeitig aus und besitzen meist ebenso viele Mail-Accounts. Um wenigstens den administrativen Aufwand zu reduzieren, stellten sie im Zuge der KDSG-Revision folgenden Rückweisungsantrag: Der Regierungsrat möge eine Bestimmung ausarbeiten, die es ihnen erlaubt, auch ihre privaten Mail-Accounts für politische Geschäfte zu nutzen und sich dienstliche Mails weiterleiten zu lassen – sofern kein übergeordnetes Recht dies verbietet. Genau das ist aber der Fall. In einer Anhörung beim Büro des Grossen Rates erklärte DSA-Leiter Ueli Buri, warum Privataccounts keine sichere Umgebung für sensible Personendaten und Staatsgeheimnisse darstellen: Etliche Parlamentarierinnen und Parlamentarier nutzen Provider wie GMX, Microsoft (Hotmail) und Google (Gmail), die den Mailverkehr ihrer KundInnen und sogar dessen Inhalte zu Werbe- und Trainingszwecken auslesen können. Auch bei anderen Anbietern ist man vor möglichen «Mitlesern» nicht gefeit, solange die E-Mails unverschlüsselt sind. Kurzum: Wer sensible Daten mit dem privaten Account empfängt oder weiterleitet, kann sie nicht vor Missbrauch schützen – und verletzt damit Artikel 18 (Absatz 3) der Kantonsverfassung, der gleichermassen für Verwaltungsbehörden wie für Parlamente gilt.

Darüber hinaus unterstehen Grossrätinnen und Grossräte dem Amtsgeheimnis. Wenn sie vertrauliche Inhalte verbreiten – und sei es nur an eine unbekannte Grösse wie Google –, machen sie sich strafbar. Weil sie im Vorfeld nicht wissen können, wer mit welchen Informationen an sie gelangt, ist auch eine automatische Weiterleitung der Dienstmails nicht zulässig.

Keine Frage: Die Pflege mehrerer Accounts und die Anwendung zusätzlicher Sicherheitsmassnahmen sind mühsam. Letztere sind aber unerlässlich zum Schutze der Bürgerinnen und Bürger, deren Interessen der Grosse Rat schliesslich vertritt. Abgesehen davon schützen sie auch die GrossrätInnen selbst davor, sich strafbar zu machen. Wie realistisch die Gefahren eines unsachgemässen Umgangs mit Daten sind, war letzten Sommer in diversen Medien zu lesen. Die Daten von 44 Schweizer Bundespolitikerinnen und Bundespolitikern waren im Darknet gelandet – weil sie ihre Dienstadressen zweckentfremdet hatten.

Vor dem Hintergrund dieser klaren Rechts- und Sachlage beschloss die Kommission für Staatspolitik und Aussenbeziehungen (SAK), das Mail-Problem auf technischem Wege anzugehen. Per Motion fordert sie den Regierungsrat zur Schaffung einer praxistauglicheren IT-Infrastruktur auf. Der Vorstoss wird voraussichtlich in der Frühlingssession des Grossen Rates behandelt.

Die zweite Lesung der KDSG-Revision blieb von dieser Diskussion unberührt.

Vorgetäuschte Überwachung? Unzulässig.

Kameraattrappen sind eine nützliche Sache. Sie kosten weniger als ihr echtes Pendant, verursachen keinen Wartungsaufwand und erfüllen trotzdem ihren Zweck: Diebstahl zu verhindern durch Abschreckung. Weil ausserdem niemand gefilmt wird, tangieren Pseudo-Kameras das Datenschutzrecht nicht. Sind sie damit eine bessere Alternative zur Videoüberwachung?

Kurz gesagt: Nein. Auch vorgetäuschte Überwachung kann dazu führen, dass Menschen ihr Verhalten anpassen und sich nicht mehr frei bewegen. Dieser sogenannte Überwachungsdruck betrifft nicht nur Kriminelle, sondern jede Person im Umfeld der Attrappe – und greift damit in ihre Rechte ein. Nicht umsonst gelten für Videoüberwachungen durch Behörden strenge Voraussetzungen, deren Einhaltung die DSA kontrolliert. Bei Attrappen fehlt diese Kontrolle, weil sie gar nicht erst unters Datenschutzgesetz fallen. Unzulässig sind sie aber auch aus einem anderen Grund: Sie verstossen gegen den Grundsatz von «Treu und Glauben». Dieses in der Bundes- und Kantonsverfassung verankerte Prinzip verpflichtet staatliche Institutionen dazu, redlich und vertrauenswürdig zu handeln – wozu das Vortäuschen falscher Tatsachen offensichtlich nicht zählt.

Deshalb verneinten wir die Frage eines Spitals, ob es Getränkeautomaten mithilfe einer Kameraattrappe oder eines Videoüberwachungs-Warnschildes vor Diebstahl schützen dürfe. Der zuständige Spitalmitarbeiter hatte den richtigen Instinkt bewiesen, indem er uns kontaktierte und die Rechtmässigkeit dieses Vorhabens prüfen liess, obwohl wir streng genommen nur für echte Überwachungen zuständig sind. Eine solche brachten wir denn auch ins Spiel: Sollten die Automaten nachweislich von Diebstahl betroffen sein, könnte eine Videoüberwachung gemäss Polizeigesetz zulässig sein. In diesem Fall ginge alles seinen

ordnungsgemässen Weg: Das Spital würde die Videoüberwachung zur Vorabkontrolle bei der KAPO und der DSA anmelden und damit die Basis für eine verhältnismässige, datenschutzkonforme – und vor allem transparente – Anti-Diebstahl-Massnahme legen.

Eine mutmassliche Zwangseinweisung

Seit einigen Jahren ist die Schweiz dabei, ein düsteres Kapitel ihrer Geschichte aufzuarbeiten: die fürsorgerischen Zwangsmassnahmen und Fremdplatzierungen in der Zeit vor 1981. Tausende Kinder und Erwachsene wurden damals Opfer von Behördenwillkür und institutioneller Gewalt. Angeregt durch die «Wiedergutmachungsinitiative» verhilft ein 2017 in Kraft getretenes Bundesgesetz Betroffenen zu ihrem Recht auf Wissen und Entschädigung. Um zu erfahren, was mit ihnen geschehen ist, können sie Einsicht in sie betreffende Akten und Dossiers beantragen. Unterstützt werden sie dabei vom kantonalen Staatsarchiv. Da es sich naturgemäss um besonders schützenswerte Personendaten handelt, ist Vorsicht geboten – erst recht, wenn nicht das Opfer selbst, sondern Angehörige die Dokumente verlangen.

Solch ein Fall beschäftigte die DSA im Frühjahr. Eine psychiatrische Klinik wollte wissen, ob sie das Dossier eines 1978 mutmasslich zwangseingewiesenen und mittlerweile verstorbenen Patienten für dessen Tochter öffnen dürfe. Zum Schutz der Klinikmitarbeiterinnen und -mitarbeiter – das Anliegen tangiert schliesslich ihr Berufsgeheimnis – empfahl die DSA dem Staatsarchiv eine gründliche juristische Abklärung. Der Klinik riet sie, vorerst keine Krankenakten herauszugeben.
Die Abklärung erfolgte wenig später in Form einer Anfrage beim Bundesamt für Justiz (BJ). Gestützt auf das «Bundesgesetz über die Aufarbeitung der fürsorgerischen Zwangsmassnahmen und Fremdplatzierungen vor 1981» befand das BJ: Betroffene und deren Nachfahren haben ein Recht auf kostenlosen und einfachen Zugang zu ihren Akten. In einem ersten Schritt sollen sie prüfen können, ob sie bzw. ihre Vorfahren tatsächlich zwangseingewiesen worden sind und wer dies aus welchem Grund veranlasst hat. Falls sich der Verdacht auf eine Zwangsmassnahme erhärtet, dürfen weitere Dossiers über die Zeit des Klinikaufenthalts herausgegeben werden. An dieser Stelle hakte die DSA nach: Kann man sich auf ein Gesetz beziehen, bevor man überhaupt weiss, ob man davon betroffen ist? In seiner Antwort empfahl das BJ unter Berücksichtigung der bundesgerichtlichen Rechtsprechung, das Gesetz zugunsten der Betroffenen auszulegen – und zwar auch der *mutmasslich* Betroffenen.

Die DSA erachtete diese Begründung als nachvollziehbar und holte noch die Meinung des fürs ärztliche Berufsgeheimnis zuständigen Gesundheitsamts ein. Letzten Endes waren sich alle Beteiligten einig: Die Tochter soll sich nach dem Schicksal ihres Vaters erkundigen dürfen.

KUW: Besondere Regelung für besondere Schulen

Kirche und Staat sind hierzulande zwar getrennt, arbeiten aber an vielen Stellen zusammen – zum Beispiel bei der kirchlichen Unterweisung (KUW). Zur Organisation ihres Religionsunterrichts sind Kirchgemeinden unter anderem auf die Klassenlisten der Volksschulen angewiesen. Deren Übermittlung ist datenschutzrechtlich kein Problem, im Gegenteil: Das Landeskirchengesetz schreibt sie sogar explizit vor. Was aber gilt für die sogenannten besonderen Volksschulen für Kinder und Jugendliche mit Beeinträchtigungen? Hier ist die Rechtslage keineswegs so eindeutig.

Im Sommer 2024 meldete sich der Leiter einer besonderen Volksschule bei uns, um diese schulintern umstrittene Frage ein für alle Mal zu klären. Eine Kirchgemeinde hatte um die Herausgabe von Klassenlisten gebeten und dabei aufs Landeskirchengesetz verwiesen. Zur Sicherheit holte die Schule noch die Einschätzung des zuständigen Amtes für Kindergarten, Volksschule und Beratung (AKVB) ein, das eine Weitergabe der Daten ebenfalls für zulässig respektive sogar für geboten hielt. Die Schulleitung indes war nicht überzeugt und wollte von uns wissen, ob die Weitergabepflicht tatsächlich auch bei den Daten vulnerabler Kinder und Jugendlicher greife. Das Ergebnis unserer Recherche: Besondere Schulen zählten noch gar nicht zu den Volksschulen, als die gesetzliche Grundlage für die Weitergaben von Klassenlisten geschaffen wurde. Sie waren Teil der Sozialhilfe und wurden erst 2022 in die Volksschulen integriert. Der Passus im Landeskirchengesetz ist deshalb nicht ohne Weiteres auf besondere Volksschulen anwendbar.

Vor allem aber haben die Personendaten ihrer Schülerinnen und Schüler eine andere Qualität. Schon die Tatsache, dass jemand eine besondere Volksschule besucht, stellt eine besonders schützenswerte Information dar.

Weil diese Lage für Kirchen und Schulen gleichermassen unbefriedigend war, erarbeitete die DSA zusammen mit den katholischen und reformierten Landeskirchen sowie mit dem AKVB eine Lösung. Diese läuft immer über die gesetzlichen Vertreterinnen und Vertreter der Kinder und Jugendlichen: Entweder werden sie über das heilpädagogische Unterweisungsangebot informiert und können sich bei Interesse selbstständig bei den Kirchgemeinden melden, oder sie stimmen von vornherein einer Datenweitergabe zu. Diese Lösung hat nun auch Einzug gehalten in die «FAQ Besonderes Volksschulangebot» und in die «Allgemeinen Vertragsbedingungen besonderes Volkschulangebot» des AKVB.

«Teams»-Beschluss: Ausdruck konstruktiver Zusammenarbeit

«M365» bietet vieles von dem, was man im Büroalltag so braucht: Tools zum Schreiben, Mailen, Präsentieren, Kalkulieren und Telefonieren. Und weil diese Anwendungen cloudbasiert laufen können, lässt sich von überall aus damit arbeiten. Das mag praktisch und effizienzsteigernd sein, birgt aber auch Gefahren: Wer Cloudservices von «M365» nutzt, gibt die tatsächliche Kontrolle über seine Daten aus der Hand. Niemand kann nachvollziehen, auf welchem seiner europaweit verteilten Server Microsoft sie verarbeitet und wer alles Zugriff darauf hat.

Trotz bekannter Risiken reüssiert «M365» zunehmend auch in öffentlichen Verwaltungen. So hat der bernische Regierungsrat 2023 beschlossen, das Softwarepaket für die gesamte Kantonsverwaltung zu beschaffen. Die DSA stellte von Beginn an klar, dass die Bearbeitung sensibler Personendaten ab Schutzniveau 2 (SN2) in der Cloud-Umgebung unzulässig ist. Entsprechend schränkte der Regierungsrat die Nutzung ein. Bestimmte Anwendungen wie «Word» oder «Outlook» (Mail) laufen im Kanton Bern nicht via Cloud, sondern im Rechenzentrum der Bedag. Für alle Cloud-Applikationen wie «OneDrive» und «SharePoint» gilt: SN2-Daten sind tabu.

Doch innerhalb der fast zweijährigen Praxis wuchs in manchen Behörden das Bedürfnis, die Regeln zu lockern. Vor allem das Telefonieren via «Teams» stellte Mitarbeitende vor Alltagsprobleme: Sollten sie auflegen, sobald die Person am anderen Ende der Leitung sensible Informationen über sich preisgibt? Letzten Herbst stand der Regierungsrat also vor der Entscheidung, «M365» auch für SN2-Daten freizugeben. Zuvor hörte er die DSA an. Unser Standpunkt aber hatte sich nicht geändert: Eine pauschale Freigabe würde die Grundrechte der Bürgerinnen und Bürger erheblich gefährden. Weil sich die Alltagsschwierigkeiten der Verwaltung vor allem auf «Teams» bezögen, sei eine Lockerung an dieser Stelle denkbar – allerdings nur beim Telefonieren und nur dann, wenn die Gespräche nicht aufgezeichnet werden. Der Regierungsrat folgte unserer Empfehlung und gab «Teams» unter den genannten Bedingungen für SN2-Daten frei (s. News-Beitrag auf der DSA-Website «Weniger Einschränkungen für ‹Teams›-Telefonie» vom 20. Oktober 2025).

Uns zeigte dieser Vorgang einmal mehr, wie kurz der Draht zwischen Regierung, Verwaltung und der DSA ist. Dass die Datenschutzbehörde angehört und ernst genommen wird, ist mit Blick auf andere Kantone keine Selbstverständlichkeit. Dieses Vertrauensverhältnis ist äusserst wertvoll und bedingt auf allen Seiten eine konstruktive Grundhaltung.

Kantonsübergreifende Krebsvorsorge – und Datenschutzberatung

Behördliche Datenbearbeitungen dürfen den ursprünglichen Zweck der Datenbeschaffung in der Regel nicht überschreiten und ihm erst recht nicht

zuwiderlaufen. Sprich: Würde die Steuerverwaltung plötzlich Gewinnspiel-Einladungen an Steuerpflichtige verschicken, so wäre das eine ziemlich klare Verletzung von Artikel 5 KDSG. Doch nicht immer ist die Auslegung des Zweckbindungsprinzips so eindeutig wie in diesem absurden Gedankenspiel. Manchmal hält die Realität buchstäbliche Grenzfälle wie den folgenden bereit:

Im Kanton Bern gibt es zwei Programme zur Brustkrebsvorsorge: «donna» und «BEJUNE». Letzteres richtet sich an Frauen im Berner Jura sowie in den Kantonen Jura und Neuenburg und beteiligt sich überdies am neuen Forschungsprojekt «BRAICS». Ziel dieses Projekts ist es, die Früherkennungsrate auch im Bereich Gebärmutterhalskrebs zu verbessern. Um Teilnehmerinnen zwischen 50 und 74 Jahren zu finden, möchte die Association pour le dépistage du cancer (ADC) BEJUNE auf ihre Adressdatenbank fürs Brustkrebsvorsorge-Programm zurückgreifen und die 6200 registrierten Personen auf das Pilotprojekt BRAICS hinweisen. Zu diesem Zweck stellte die ADC einen Antrag an die drei betroffenen Kantone und liess diesen in Kopie auch den Datenschutzbeauftragten der Kantone Bern und Jura/Neuenburg zukommen. Die Genehmigung fürs eigentliche Forschungsprojekt durch die zuständige Ethikkommission lag zu diesem Zeitpunkt noch nicht vor. Gleichwohl nutzten die Datenschutzbeauftragten ihren kurzen Draht zueinander und tauschten sich über das Vorhaben aus. Beide kamen zum Ergebnis, dass es sich dabei nicht um eine Zweckentfremdung der Datenbank handeln würde. Erstens verfolgten beide Programme das gleiche Ziel: Krebsvorsorge bei einer klar definierten Personengruppe. Zweitens wolle die ADC keine Daten an BRAICS weitergeben, sondern lediglich Einladungen zur Projektteilnahme versenden. Die Datenschutzbehörden hiessen den Vorgang deshalb gut – unter der Voraussetzung, dass die kantonalen Gesundheitsdirektionen diese Ansicht teilen und dass die zuständige Ethikkommission das Forschungsprojekt genehmigt.

Fazit 1: Es lohnt sich, die Datenschutzbehörden frühzeitig ins Boot zu holen.
Fazit 2: Das schweizweite Datenschutz-Netzwerk durch den Verband privatim zahlt sich auch im Kleinen aus.

6.2 Beratung betroffener Personen

Strafvollzug: Wenn Briefe mitgelesen werden

Unsere Grundrechte sind unantastbar? Nicht ganz. Zur Organisation des gesellschaftlichen Miteinanders muss der Staat sie immer wieder einschränken. Das offensichtlichste Beispiel hierfür ist die Haftstrafe: Wer für ein Verbrechen verurteilt wurde, verwirkt vorübergehend sein Recht auf Freiheit – nicht aber alle anderen. Der Delinquent bleibt auch dann Rechtsträger, wenn er die Schwelle zur

Justizvollzugsanstalt (JVA) überschritten hat. Zum Beispiel kann er nach wie vor Akteneinsicht beantragen oder sich für den Schutz seiner Daten einsetzen.

Einem im Kanton Bern Inhaftierten ist dies sehr bewusst. Mehrfach hat er sich schon an die DSA gewandt, um Rechtsauskunft oder Vermittlung zu erhalten – und in einigen Fällen konnten wir ihm zu seinem Recht verhelfen. Letztes Jahr beklagte er sich unter anderem darüber, dass die JVA seine Post kontrolliert habe. Die entsprechende Verfügung der JVA schickte er dankenswerterweise gleich mit. Aus dieser ging hervor, dass es für die Briefkontrolle erstens eine Rechtsgrundlage gibt und dass diese zweitens im konkreten Fall auch greift.

Zwar dürfen Gefängnisinsassen Kontakt zur Aussenwelt halten. Die JVA muss aber dafür sorgen, dass daraus keine Gefahr entsteht – weder für die Haftanstalt selbst noch für den Vollzugserfolg des Insassen. Der Umgang mit falschen Personenkreisen könnte schliesslich dessen Rückfallrisiko erhöhen. Gemäss JVA trugen einige Briefe des Betroffenen verdächtige Symbole und mussten deshalb geprüft werden.

Als Datenschutzbeauftragte sahen wir keinen Anlass, den Ausführungen der JVA zu misstrauen. Dem Insassen gegenüber stellten wir klar: Grundrechte können eingeschränkt werden, wenn dies auf einer hinreichenden gesetzlichen Grundlage beruht und im öffentlichen Interesse liegt. Beides ist aus den oben genannten Gründen der Fall. Auch muss die Einschränkung verhältnismässig sein, was ebenfalls zutrifft: Die JVA kontrolliert eingehende Briefe nicht systematisch, sondern im konkreten Verdachtsfall. Sie fertigt dann eine Sicherheitskopie an, informiert den Insassen darüber und gibt ihm das Original zurück – aus unserer Sicht die denkbar behutsamste Form einer Briefkontrolle.

Weiss der Smartmeter zu viel?

Viele Schweizer Haushalte haben in den letzten Monaten einen neuen «Mitbewohner» bekommen: den Smartmeter. Das Gerät verspricht maximale Transparenz über den eigenen Stromverbrauch und soll helfen, diesen effizienter zu steuern. In regelmässigen Abständen sendet es Werte an den Energieversorger, die auch vom Verbraucher/von der Verbraucherin selbst eingesehen werden können.

Der Einbau des Smartmeters geschieht nicht nur freiwillig: Gemäss Stromversorgungsgesetz müssen bis Ende 2027 80 Prozent der Haushalte in einem Netzgebiet damit ausgestattet sein. Aktuell sind es schweizweit mehr als 50 Prozent. Mit seiner wachsenden Verbreitung ist der Smartmeter allerdings auch zunehmend Kritik ausgesetzt. Ein Bürger zog wegen datenschutzrechtlicher Bedenken bis vors Bundesverwaltungsgericht, wurde dort aber abgewiesen. Das Gericht beurteilte den Einsatz von Smartmetern als rechts- und datenschutzkonform. Die Art der Datenerhebung und der Daten selbst liessen keine detaillierten Rückschlüsse auf das Verhalten der Betroffenen oder auf den Einsatz bestimmter Geräte zu. Auch würden die Daten nicht zum Zwecke eines Profilings erhoben, sondern für die

Abrechnung sowie zur Steuerung des Netzbetriebs. Die dadurch angestrebte Effizienzsteigerung liege überdies im öffentlichen Interesse.

Diese Auffassung teilt auch die DSA, die im Berichtsjahr mit dem Thema zu tun bekam. Binnen weniger Wochen meldeten sich gleich zwei Bürger bei uns. Einer zog die Rechtmässigkeit des Systems insgesamt in Zweifel. Weder wolle er seine tagesaktuellen Verbrauchsdaten wissen noch solle irgendwer diese Daten sammeln. Wir verwiesen auf das Gerichtsurteil, demzufolge die intelligente Stromdatenmessung recht-, zweck- und verhältnismässig geschieht.

Die zweite Bürgeranfrage wandte sich nicht gegen den Smartmeter als solchen, sondern gegen die Häufigkeit der Datenübermittlung. Auf der Website seines Energieversorgers habe der Betroffene gelesen, dass die Verbrauchsdaten des Smartmeters viermal pro Tag ausgelesen würden. Diese Frequenz sei von der Stromversorgungsverordnung nicht gedeckt. Also erkundigten wir uns beim betreffenden Energieversorger, was es mit der häufigen Datenübermittlung auf sich habe. Dessen Antwort überzeugte uns: Der Smartmeter sende die Werte nicht viermal am Tag an den Energieversorger, sondern an einen sogenannten Datenkonzentrator. Die Regelmässigkeit dieser Übertragung solle das System vor witterungsbedingt oder anderweitig verfälschten Werten schützen. Auch geschehe die Übertragung vorderhand nur zwischen zwei technischen Einheiten: dem Smartmeter und dem Konzentrator. Währenddessen seien die Daten verschlüsselt und pseudonymisiert und liessen sich keinen bestimmten Personen zuordnen. Der Energieversorger selbst rufe die Werte nur einmal am Tag ab und halte sich somit an die gesetzlichen Vorgaben.

Geschwärzte Passagen in Polizeiakten schüren Misstrauen

Einsicht in die eigenen Daten zu erhalten, ist zweifellos ein Grundrecht. Weniger klar ist, wie weit diese Einsicht im Einzelfall gehen muss. Stehen sich die Interessen einer Privatperson und einer Behörde gegenüber, braucht es zuweilen eine Schlichterin. Als solche trat die DSA im Mai auf.

Ein wegen Sachbeschädigung verurteilter Bürger stand damals im Austausch mit der KAPO. Weil er Unstimmigkeiten zwischen Zeugenaussage und Einsatzprotokoll witterte und nach wie vor von seiner Unschuld überzeugt war, verlangte er Einblick in die polizeiinternen Einträge zu seinem Fall. Die bekam er auch – aber zu zwei Dritteln geschwärzt. Die KAPO begründete ihr Vorgehen damit, dass die verdeckten Passagen Rückschlüsse auf ihre Einsatztaktik zuliessen und dadurch die Polizeiarbeit gefährden könnten. Dass auf den Dokumenten praktisch nichts Zusammenhängendes zu erkennen war, nährte das Grundmisstrauen des Bürgers jedoch zusätzlich. Also wandte er sich an die DSA.

Um uns ein Bild von der Lage zu machen, baten wir die KAPO um die unzensierten Dokumente (das ist insofern unproblematisch, als die DSA einer strengen Verschwiegenheitspflicht untersteht). Unsere Einschätzung: Ein Grossteil der

versteckten Passagen ist für den Betroffenen zwar uninteressant, aber auch entsprechend harmlos. Wir empfahlen der KAPO deshalb, die Schwärzungen auf ein Minimum zu reduzieren und damit das Vertrauen des Bürgers wiederherzustellen. Unseren eigenen Schwärzungsvorschlag schickten wir gleich mit. Die KAPO war damit einverstanden, der Bürger zufrieden und eine Eskalation mit kleinem Aufwand vermieden.

Die Grenzen unserer Möglichkeiten bei der Akteneinsicht

Wem kann die DSA helfen – und auf welche Weise? In unserem Arbeitsalltag werden wir immer wieder mit unseren Grenzen konfrontiert. Oft verirren sich Anfragen zu uns, für die wir nicht zuständig sind und die wir höchstens mit allgemeinen Hinweisen beantworten dürfen. In anderen Fällen sind wir zwar die richtige Anlaufstelle, wird aber unsere Handlungsmacht überschätzt. So geschehen im August 2025: Ein Bürger verlangte Einsicht in die Akten eines unter Beistandschaft stehenden Altersheimbewohners, der ihm eine Generalvollmacht erteilt hatte. Nach Rücksprache mit einer Fachperson erklärte die KESB diese Vollmacht jedoch für ungültig und verweigerte die Akteneinsicht. Der Betroffene habe mangels Urteilsfähigkeit überhaupt keine Vollmacht ausstellen können.

Der fragliche Bevollmächtigte akzeptierte diesen Beschluss nicht und wandte sich mit einer aufsichtsrechtlichen Anzeige an uns. Er verlangte, die Gültigkeit der Vollmacht anzuerkennen und die KESB zur Aktenauskunft zu verpflichten. Dies jedoch steht uns nicht zu. Wir konnten lediglich prüfen, ob die KESB das Auskunftsrecht des Bürgers verletzt hat. Auf Grundlage der vorhandenen Informationen gingen wir allerdings davon aus, dass er kein Auskunftsrecht besitzt und die KESB datenschutzrechtlich korrekt gehandelt hat. Die Grundlagen dieser Einschätzung – also den Entscheid über die Urteilsfähigkeit des Heimbewohners und die Gültigkeit seiner Vollmacht – können und dürfen wir nicht beurteilen. Auch können wir der KESB keine Anweisungen erteilen. Unser Handlungsspielraum erschöpft sich in der Beratung des Bürgers und im Hinweis darauf, dass er die Verfügung anfechten kann – und das hat er ohnehin schon getan.

Ungebetene Vereinspost – in der Regel zulässig

Wer einmal den Wohnort gewechselt hat, kennt das Phänomen: Plötzlich liegt Post von Clubs oder Parteien im Briefkasten, mit denen man bis dato nichts zu tun hatte. Oder der kürzlich erst geborene Nachwuchs wird zur Waldspielgruppe eingeladen. Dahinter stecken in aller Regel Listenauskünfte – also nach bestimmten Kriterien wie Alter oder Geschlecht geordnete Einwohnerdaten, die Gemeinden auf Anfrage zur Verfügung stellen.

Doch nicht immer sind die Bürgerinnen und Bürger damit einverstanden. Im vergangenen Jahr meldeten sich mehrere Betroffene irritiert bei der DSA: Sie hätten einer Weitergabe ihrer Daten nie zugestimmt. Der guten Form halber

wiesen wir sie darauf hin, dass wir (noch) nicht für kommunale Körperschaften zuständig sind. Weil derlei Anfragen aber mit einer gewissen Häufigkeit eintreffen, erklären wir den Betroffenen zumindest die allgemeine Rechtslage. Und die ist eigentlich klar: Gemeinden dürfen Einwohnerdaten an Private weitergeben, sofern diese ein schützenswertes Interesse glaubhaft machen. Ein solches Interesse kann zum Beispiel sein, die kulturelle Vielfalt des Ortes aufrechtzuerhalten. Insofern dürfen auch Sportvereine, Trachtengruppen oder andere Organisationen ohne kommerzielle Absichten mit Einwohnerdaten beliefert werden. Systematische Bekanntgaben wie Listenauskünfte bedürfen allerdings einer Rechtsgrundlage im Gemeindereglement. Auch auf die Art der Daten kommt es an: Name, Vorname, Geschlecht, Adresse, Zivilstand, Heimatort sowie Datum des Zu- und Wegzugs sind normalerweise erlaubt – es sei denn, die Adresse lautet beispielsweise auf ein Gefängnis. Sensible Informationen wie Verwandtschaftsverhältnisse oder Konfessionen sind von vornherein tabu.

Ob eine Gemeinde im Einzelfall korrekt gehandelt hat, beurteilen wir aus erwähnten Gründen (noch) nicht. Stattdessen verweisen wir die Betroffenen an die zuständige kommunale Aufsichtsstelle – und auf die Möglichkeit einer Datensperre, die für Listenauskünfte nicht einmal begründet werden muss.

Ein Betroffener – zwei gegenläufige Interessen

Kein Grundrecht gilt absolut. Das wird uns spätestens bewusst, wenn wir nach Mitternacht in einem Mietshaus Blockflöte üben oder auf einem Privatgrundstück parkieren wollen. Unsere Freiheit endet in der Regel dort, wo die der anderen beginnt. So einleuchtend das auf den ersten Blick auch ist – in der Praxis stellt das Austarieren von Grundrechten die drei Staatsgewalten regelmässig vor Herausforderungen. Besonders kompliziert wird’s, wenn zwei Rechte ein und derselben Person miteinander im Konflikt stehen.

Ein (nicht ganz alltägliches) Beispiel aus dem DSA-Alltag: Anfang Juni meldete ein Bürger eine potenzielle Datenschutzverletzung. Er habe dem AGR konkrete Fragen zu einem Einzonungsverfahren gestellt und um Akteneinsicht gebeten. Das AGR habe ihn daraufhin an die Gemeinde als zuständige Auskunftsstelle verwiesen und seine E-Mail gleich an deren Bauverwalter weitergeleitet – aus Sicht des Bürgers ein klarer Fall unzulässiger Datenweitergabe. Besonders heikel sei das, weil der Bauverwalter in ein Beschwerdeverfahren zu einem Bauprojekt in der betroffenen Zone involviert sei. Hat das AGR also einen Fehler gemacht? Nein, lautet das Fazit der DSA nach sorgfältiger Prüfung des E-Mail-Verkehrs und der gesetzlichen Grundlagen. Im Gegenteil: Das Amt *musste* die Anfrage sogar weiterleiten.

Konkret standen sich in diesem Fall zwei Interessen des Bürgers gegenüber: sein Recht auf Information und sein Recht auf informationelle Selbstbestimmung (= Datenschutz). Gemäss dem kantonalen Gesetz über die Information und die Medienförderung müssen Behörden über Tätigkeiten von öffentlichem Interesse – worunter eine Zonenplanrevision zweifellos fällt – informieren und die zugehörigen Unterlagen auf Anfrage zugänglich machen. Als Genehmigungsbehörde hat das AGR diese Unterlagen zwar geprüft und bearbeitet. Erstellt wurden sie aber von der Gemeinde, weswegen *sie* auch für deren Herausgabe zu sorgen hat.

Gleichwohl musste das AGR reagieren: Die Informations- und Medienverordnung verpflichtet Behörden dazu, Informationsgesuche umgehend zu prüfen und weiterzuleiten, falls sie selbst nicht zuständig sind. Dass auf diesem Wege auch Personendaten weitergegeben werden – namentlich die Mail-Adresse des Bürgers –, stellt per se noch keine Datenschutzverletzung dar. Dies wäre erst der Fall, wenn «besonders schützenswerte private Interessen» der Weitergabe entgegenstünden.

Hatte das AGR Anlass, von «besonders schützenswerten Interessen» des Betroffenen auszugehen? Nach unserer Auffassung nicht. Der Hinweis auf ein hängiges Beschwerdeverfahren unterstreicht eher sein Interesse an Akteneinsicht als jenes am Schutz seiner Daten. Hätte das AGR den Bürger vor dem Weiterleiten seiner E-Mail um Erlaubnis bitten müssen? Dann müsste es das theoretisch bei jeder Anfrage dieser Art tun – aus unserer Sicht ein unverhältnismässiger Aufwand, der mit der Pflicht zur Weiterleitung an die zuständige Behörde gerade vermieden werden soll.

6.3 Formelle Stellungnahmen

In vielen Gesetzesvorhaben spielt Datenschutz eine Rolle, doch nicht immer drängt sich der Zusammenhang auf Anhieb auf. Die DSA ist deshalb dankbar, automatisch auf jedes kantonale Vernehmlassungsverfahren hingewiesen zu werden. So können wir uns selbst ein Bild machen und nötigenfalls Stellung nehmen, um potenzielle Fallstricke frühzeitig zu benennen. Auch in den verwaltungsinternen Mitberichtsverfahren äussern wir uns, sofern wir datenschutzrechtliche Schwierigkeiten oder Unklarheiten ausmachen. In Vernehmlassungen auf Bundesebene wirken wir indirekt mit, wenn der Regierungsrat unsere Anmerkungen in seine Stellungnahme einfliessen lässt.

Zu manchen Gesetzesvorhaben oder Regierungsratsbeschlüssen können wir uns auf Einladung mündlich äussern (z. B. im Rahmen einer Anhörung).

Idealvorlage in eigener Sache: das neue KDSG

Dass wir uns zu einer Vorlage äussern können, die uns selbst unmittelbar betrifft, kommt nicht oft vor. Die KDSG-Revision war uns deshalb besonders wichtig. Sie berührt das Fundament unseres Schaffens und hat massive Auswirkungen auf unseren Arbeitsalltag (s. Ziffer 2). Entsprechend zufrieden sind wir mit dem Ergebnis der parlamentarischen Beratungen: Das Gesetz ist in seiner Idealform angenommen worden. Dies haben wir u. a. der SAK zu verdanken, die all unseren Empfehlungen gefolgt ist und diese sehr überzeugend im Grossen Rat vertreten hat. Leicht gemacht hat es sich die Kommission dabei keineswegs. Sie hat die vielen Änderungs- respektive Rückweisungsanträge sorgfältig geprüft und die DSA dazu angehört. Zwei Wünsche, die wir Ende 2024 vorgebracht hatten (s. Jahresbericht 2024, Ziffer 6.2), hat die SAK heuer berücksichtigt und in der ersten Lesung durchgebracht. Vor der zweiten Lesung lud die Kommission uns wiederum zu einer Anhörung ein. Unsere wichtigste Botschaft ist dabei zweifellos angekommen: Die Grundsätze des Datenschutzrechts stehen in der Kantonsverfassung und bleiben unverändert. Das neue KDSG ist nicht strenger, sondern präziser als das bisherige. Dass sich insbesondere die Gemeinden vor einer Verschärfung des Datenschutzes fürchten, ist verständlich. Dem Datenschutz ist tatsächlich mehr Aufmerksamkeit zu schenken – aber nicht als Folge der KDSG-Revision, sondern der Digitalisierung selbst. Es sind die rasanten Entwicklungen im IT-Bereich und die immer unverfrorener agierenden Cyberkriminellen, die die Schutzanforderungen erhöhen.

Und was unsere künftige Zuständigkeit für die Gemeinden betrifft, so sind wir überzeugt: Beide Seiten können nur davon profitieren. Die Gemeinden bekommen unsere Unterstützung für Pflichten, die sie gemäss bestehendem KDSG heute schon haben. Im Gegenzug lernen wir die alltäglichen Probleme und Bedürfnisse der Gemeinden kennen – und damit noch mehr Anwendungsfälle des vielseitigen Themas Datenschutz, zu dem auch wir nie ausgelernt haben werden.

Wenn Bundesangestellte Kantonsaufgaben übernehmen – und umgekehrt

Während Sie im verspäteten ICE sitzen, ist es Ihnen vermutlich egal, wer da gerade Ihren Nachbarn kontrolliert: eine Bahnmitarbeiterin, eine Kantons- oder eine Bundesbeamtin. Was aber, wenn diese als Nächstes Ihren Ausweis verlangt, ihn fotografiert und in einer WhatsApp-Chatgruppe teilt? Spätestens hier ist die Frage, für wen die Kontrolleurin arbeitet, nicht mehr so trivial. Sie entscheidet darüber, ob sich der EDÖB oder die DSA um den Vorfall kümmert.

Bekanntlich liegt die Polizeihoheit beim Kanton. Sprich: Für die Sicherheit der Bevölkerung ist der jeweilige Kanton zuständig. An Grenzübergängen oder in Fernzügen sind es jedoch oft Beamte des Bundesamts für Zoll und Grenzsicherheit (BAZG), die Schutz- und Kontrollfunktionen wahrnehmen. Dies

geschieht auf der Grundlage einer Zusammenarbeitsvereinbarung zwischen Bund und Kantonen. Im Jahr 2025 wurde die DSA zur Erneuerung des Abkommens mit dem Kanton Bern konsultiert. Uns fiel direkt auf, dass sich das Dokument sowohl aufs kantonale als auch aufs eidgenössische Datenschutzgesetz abstützt. Das ist mindestens ungünstig, weil sich im Zweifelsfall weder der EDÖB noch die DSA zuständig fühlen. Es erschien uns aber auch als falsch: Eine kantonale Aufgabe bleibt selbst dann eine kantonale Aufgabe, wenn eine Bundesbeamtin sie ausübt. Und wer im kantonalen Auftrag handelt, fällt unter das KDSG. Erst im Nachhinein erfuhren wir, dass ein neues Bundesgesetz dem BAZG ausdrücklich erlauben wird, kantonale polizeiliche Aufgaben zu übernehmen und in der Vereinbarung mit dem Kanton den Datenschutz zu regeln. Deshalb fragten wir den EDÖB an, ob er sich für die Aufsicht als zuständig erachtet. Sofern er dies bejaht, ist die Angelegenheit für uns erledigt.

Auch im Bereich Geldspiel arbeiten Bund und Kantone zusammen – allerdings unter umgekehrten Vorzeichen. Wenn ein Spielbankbetreiber zu lasch kontrolliert oder unbewilligte Automaten aufstellt, ist das ein Fall für die Eidgenössische Spielbankenkommission (ESBK). Die Bundesbehörde ist für die Strafverfolgung in diesem Bereich zuständig, kann sich aber von KAPO-Mitarbeitenden unterstützen lassen. Diese Form des «Personalverleihs» ist ebenfalls in einer Vereinbarung geregelt. Im Berichtsjahr sollte eine zugehörige Verordnung geändert werden: KAPO-Mitarbeitende, die im Dienste der ESBK eingesetzt werden, sollten für diese Aufgabe Zugang zur kantonalen Personendatenbank GERES erhalten. Doch die DSA wies das Vorhaben als unzulässig zurück. Sobald ein Kantonsangestellter Bundesaufgaben übernimmt, handelt er als Teil der Bundesbehörde. Als solcher kann er keinen pauschalen Zugriff auf eine Datenbank erhalten, die der Gesetzgeber explizit für kantonale Aufgaben geschaffen hat.

Anonym oder pseudonym? – Kleinigkeiten mit grosser Tragweite

Die schweizerische Gesundheitspolitik steht vor einem einschneidenden Systemwechsel. Wenn das revidierte Transplantationsgesetz in Kraft tritt, gilt fortan die Widerspruchslösung. Das heisst: Wer keine Organe spenden will, muss dies aktiv kundtun. Weil der Tod zum Existenziellsten und Intimsten eines Menschen gehört, ist bei der Umsetzung dieser Gesetzesänderung grösste Vorsicht geboten – insbesondere im Hinblick auf den Datenschutz. Entsprechend intensiv befasste sich die DSA mit den zugehörigen Verordnungen. Im Mitberichtsverfahren beantragten wir gegenüber dem Regierungsrat zahlreiche Änderungsvorschläge bzw. Hinweise, die dieser an den Bund richten möge. Einer davon betraf die Unterscheidung zwischen anonymisierten und pseudonymisierten Daten. Was auf den ersten Blick nach einer juristischen Spitzfindigkeit aussieht, ist in der Praxis entscheidend: Werden Daten *anonymisiert*, so sind sie dauerhaft unkenntlich gemacht. Niemand kann mehr einen Bezug zu einer konkreten Person herstellen. *Pseudonymisierte* Daten sind zwar ebenfalls unkenntlich gemacht, können aber mithilfe eines «Schlüssels» wieder auf

konkrete Personen rückschliessen lassen. Ein Beispiel hierfür wäre eine Datenbank, in der Patientinnen und Patienten nicht mit Namen und Adressen, sondern mit AHV-Nummern hinterlegt sind. AHV-Nummern sind ein klarer Identifikator, den es bei anonymisierten Daten nicht geben darf. Weil in den Verordnungen zum Transplantationsgesetz keine echte Anonymisierung vorgesehen ist, beantragten wir, überall den Begriff «anonymisiert» durch «pseudonymisiert» zu ersetzen.

Auch bei den Zuständigkeiten fürs Transplantationsregister beantragten wir Nachbesserungen. Die Verantwortung sollte bei *einem* Akteur liegen und nicht auf mehrere Behörden verteilt werden. Erstens dient das der Nachvollziehbarkeit staatlichen Handelns, zweitens hilft es betroffenen Bürgerinnen und Bürgern, ihre Rechte bei der zuständigen Behörde geltend zu machen.

Ferner beantragte die DSA, in allen Verordnungen das Wort «erforderlich» durch «unentbehrlich» zu ersetzen. Hintergrund ist das Datenschutzrecht auf Bundes- und Kantonsebene: Wenn der Staat sensible Personendaten bearbeitet, so muss dies zur Erfüllung seiner Aufgabe «zwingend erforderlich» oder «unentbehrlich» (und nicht nur praktisch) sein – also im Grunde alternativlos. Auch das mag wie ein kleines Detail wirken, ist aber erstens Gesetz und kann zweitens im Einzelfall den Unterschied machen.

Der Regierungsrat hat die erwähnten und alle weiteren Anträge der DSA berücksichtigt und sie in seine Vernehmlassungsantwort an den Bund aufgenommen.

Gesundheitsplattform: Stossrichtung klar, Zuständigkeiten nicht

Im September konnten wir uns zu einem viel beachteten gesundheitspolitischen Vorhaben äussern: der Teilrevision des Spitalversorgungsgesetzes. Sämtliche Listenspitäler des Kantons Bern sollen künftig die gleiche Software verwenden. Ein einheitliches Klinikinformationssystem soll die jeweiligen Einzellösungen ersetzen und eine neue «Gesundheitsplattform» den Datenfluss erleichtern. Die Hoffnung dahinter: Wenn die Spitäler besser vernetzt sind, können sie effizienter zusammenarbeiten. Was auf den ersten Blick einleuchtet, birgt bei näherer Betrachtung so manchen Fallstrick.

Bei der Einführung neuer Software stellt sich zwangsläufig die Frage nach dem Datenschutz – erst recht im Gesundheitswesen, wo fast jedes Personendatum besonders schützenswert ist. Eine gemeinsame Gesundheitsplattform kann die Sicherheit dieser Daten sogar erhöhen, weil sie Umwege via Telefon oder E-Mail unnötig macht und es im Zweifel einfacher ist, *ein* System zu schützen als zehn verschiedene. Dafür müssen allerdings die Voraussetzungen stimmen – angefangen bei einer klaren Rollenverteilung. Damit die DSA die Einhaltung des Datenschutzgesetzes und die Sicherheit einer solchen Gesundheitsplattform prüfen kann, muss sie wissen, wer diese überhaupt betreibt. Die GSI? Das Inselspital? Im bisherigen Gesetzentwurf fehlt eine eindeutige Bezeichnung der Trägerschaft,

wie wir in unserer Vernehmlassungsantwort festgehalten haben. Ausserdem wird nicht klar, ob die Gesundheitsplattform eine Art Datenbank sein soll oder lediglich für den Transfer gedacht ist.

Derlei Fragen sind keine Haarspalterei – sie sind essenziell. Erst auf Grundlage einer klaren Zuständigkeits- und Funktionsbeschreibung lassen sich weitere datenschutzrelevante Fragen prüfen. Zum Beispiel jene nach dem Anbieter der Software und dessen Möglichkeit, auf Patientendaten zuzugreifen: Die geplante Zusammenarbeit mit dem US-Konzern Epic ist durchaus umstritten, wie mehrere Vernehmlassungsantworten und ein Grossratsvorstoss zeigen.

Die DSA wird den weiteren Verlauf des Gesetzgebungsverfahrens deshalb aufmerksam begleiten.

6.4 Vorabkontrollen

Plant eine Behörde eine neue elektronische Datenbearbeitung, so muss sie unter bestimmten Bedingungen die DSA beiziehen. Neu sind Datenbearbeitungen zum Beispiel dann, wenn bestimmte Prozesse digitalisiert werden, wenn bestehende Software ersetzt wird oder wenn Daten zu einem neuen Zweck erhoben werden (meist infolge einer Gesetzesänderung). Derlei Projekte müssen uns zur Vorabkontrolle vorgelegt werden – vorausgesetzt, sie betreffen einen grösseren Personenkreis und sind mit erhöhten Risiken verbunden. Letzteres ist der Fall, wenn es um besonders schützenswerte/geheimhaltungspflichtige Daten geht oder wenn die eingesetzte Technik Risiken birgt (z. B. bei Cloud-Computing oder KI-Bots). Auch Videoüberwachungen sind in der Regel vorabkontrollpflichtig.

Die Verfahren sind mehr oder minder komplex und nehmen deshalb unterschiedlich viel Zeit in Anspruch. Oft braucht es mehrere Durchläufe (Iterationen), bis wir ein Projekt final beurteilen können. Im Folgenden skizzieren wir fünf Vorabkontrollgeschäfte, die entweder aus inhaltlichen oder aus verfahrenstechnischen Gründen interessant sind.

«NFFS»: besonders dynamisch, besonders intensiv

Besondere Umstände erfordern besondere Massnahmen – so könnte das Motto der DSA für die Vorabkontrolle des «Neuen Fallführungssystems» («NFFS») lauten. Besonders ist das «NFFS» erstens durch seine Reichweite: Die Software soll in 85 Behörden mit mehr als 2000 Anwenderinnen und Anwendern zum Einsatz kommen. Primär geht es darum, die Fallführung in den Sozialdiensten zu vereinheitlichen; später sollen auch die KESB sowie die Arbeitsintegration damit

arbeiten. Mit dieser grossen Reichweite geht einher, dass zwei kantonale Direktionen (GSI, DIJ) und zwei föderale Ebenen (Kanton, Gemeinden) sowie zwei IT-Unternehmen in das Projekt involviert sind. Besonders ist zweitens dessen Zeitplan: Bevor «NFFS» flächendeckend eingeführt wird, sollen ausgewählte Sozialdienste es bereits im Pilotbetrieb testen.

Diese Besonderheiten bewogen uns dazu, im Rahmen unseres gesetzlichen Spielraums vom üblichen Vorabkontrollverfahren abzuweichen. Auf Wunsch der GSI zogen wir die Prüfung eines einzelnen Projektteils vor, der die Datenmigration für den Pilotbetrieb vorbereitet. Um nämlich die Daten aus den alten Fallführungssystemen ins neue überführen zu können, muss man sie zunächst analysieren und in ein «NFFS»-kompatibles Zwischenformat bringen. Im November 2024 erhielten wir die Unterlagen für dieses Teilvorhaben und wenig später die eingeforderten Nachbesserungen, sodass wir bereits im Januar 2025 grünes Licht geben konnten.

Anschliessend lief die Vorabkontrolle des Gesamtprojekts weiter – und zwar ebenso flexibel. Die erste Iteration schlossen wir ab, obwohl noch wichtige Unterlagen fehlten. Unsere Befunde dazu übermittelten wir den Projektverantwortlichen zeitnah, sodass sie die Verbesserungsarbeiten noch vor Eintreffen unseres ersten Abschlussberichts in Angriff nehmen konnten. In dieser Dynamik und in ähnlich straffer Taktung verliefen auch die zweite und dritte Iteration. Mit unserer Zusage durften die Pilot-Sozialdienste «NFFS» in Betrieb nehmen, noch bevor das Verfahren offiziell beendet wurde. Bedingung: Wesentliche Mängel mussten zuvor behoben werden. Dass die Pilotphase dennoch erst im Dezember begann, hat projektinterne Gründe.

Dank dieser beiderseits flexiblen Vorgehensweise konnte das Projekt laufend weiterentwickelt werden, ohne dass es zu wochen- oder monatelangen Marschhalten kam. Andererseits wurde das Verfahren dadurch umso komplexer, erforderte zahllose Absprachen und eröffnete mehrere Seitenstränge. Einer davon betraf das kantonale Login-System auf Grundlage der Bundeslösung AGOV. Zwischen GSI, DSA und KAIO herrschten unterschiedliche Auffassungen zum erforderlichen Sicherheitslevel. Aus unserer Sicht müssen sich Mitarbeitende zwingend mithilfe eines Ausweisdokuments identifizieren, sofern sie mit sensiblen Personendaten zu tun haben. Bis sich alle Beteiligten darauf einigen konnten, gingen mehrere Wochen ins Land. Damit die Pilot-Sozialdienste gleichwohl ihre Arbeit mit «NFFS» aufnehmen konnten, erlaubten wir übergangsweise ein geringeres Sicherheitslevel. Das Risiko erachteten wir als tragbar, da es sich um nur zwei Sozialdienste und um eine geringe Zeitspanne handelte. Im Nebeneffekt hat die AGOV-Diskussion dazu geführt, dass der Sicherheitsstandard künftig auf den ganzen Kanton ausgedehnt wird.

Alles in allem halten wir fest: «NFFS» war eines unserer intensivsten Vorabkontrollprojekte überhaupt. Dass es erfolgreich und zeitnah abgeschlossen werden konnte, liegt an der oben beschriebenen Dynamik – und die war nur möglich, weil die DSA von Anfang an einbezogen wurde.

Die Nacharbeiten (Erledigung der Restpendenzen seitens GSI und anschliessende Prüfung durch die DSA) sind noch im Gang.

Chatbot: keine Personendaten, kein Problem

«Ich lebe seit drei Jahren in der Schweiz, fahre aber immer noch mit meinem spanischen Führerausweis durch die Gegend. Muss ich mit Sanktionen rechnen?» «Ja, es könnten Sanktionen auf Sie zukommen, da der ausländische Führerausweis innerhalb von 12 Monaten nach Einreise in die Schweiz in einen Schweizer Führerausweis umgetauscht werden muss.» Wer hier so unmissverständlich die Rechtslage erklärt, ist kein Mensch, sondern ein Chatbot. Er steht seit diesem Jahr in den Diensten des kantonalen Strassenverkehrs- und Schifffahrtsamtes (SVSA) und beantwortet allerlei themenbezogene Fragen. Auskünfte über Dritte – zum Beispiel, wer hinter einer bestimmten Kontrollnummer steckt – verweigert er hingegen mit Verweis auf den Datenschutz. Dies ist nur eine von vielen Vorkehrungen, die das SVSA zur sicheren Einführung des Chatbots getroffen hat. Eine weitere zeigt sich gleich zu Beginn des «Gesprächs». Bevor man zu tippen beginnt, wird man darum gebeten, keine personenbezogenen Daten oder vertraulichen Informationen einzugeben. Dass derselbe Hinweis auch beim Telefonat mit dem SVSA-Voicebot ertönt, geht auf die DSA zurück.

Sowohl der Chat- als auch der Voicebot wurden letztes Jahr als Gesamtprojekt vorabkontrolliert. Auf den ersten Blick handelt es sich hier zwar nicht um eine Datenbearbeitung im eingangs dieses Kapitels beschriebenen Sinne. Die Bots sollen schliesslich keine Personendaten sammeln, sondern Fragen beantworten. Damit sie aber gar nicht erst an Personendaten gelangen, braucht es einen klaren Hinweis an die Nutzerinnen und Nutzer. Dieser war ursprünglich nur für den Chatbot vorgesehen, wurde aufgrund unserer Empfehlung aber auch dem Voicebot vorangestellt.

Ebenfalls nachbessern musste das SVSA in puncto Handynummern: Auf Wunsch erhalten Anruferinnen und Anrufer per SMS eine Zusammenfassung des Gesprächs und weiterführende Info-Links. Zu diesem Zweck muss der Bot kurzzeitig Mobiltelefonnummern bearbeiten. Gemäss Projektkonzept sollten diese fünf Tage aufbewahrt und in der Cloud gespeichert werden – aus unserer Sicht unnötig und riskant, weil die Gespräche dadurch bestimmten Personen zugeordnet werden könnten. Eine Weitergabe der Nummern an den Cloudservice hätte überdies bedingt, dass die Subunternehmen Microsoft und Google diese Datenbearbeitung detailliert dokumentieren und erst das SVSA und anschliessend die DSA die Unterlagen prüfen. Dies hätte das Verfahren ohne Not verkompliziert und verlängert. In Absprache mit seinem Softwareanbieter änderte das Amt die Aufbewahrungsfrist: Die Telefonnummern werden nun direkt nach dem SMS-Versand gelöscht.

Weil es von vornherein nur wenig zu beanstanden gab und das SVSA umgehend die geforderten Nachbesserungen vorgenommen hat, konnte die Vorabkontrolle

binnen weniger Wochen abgeschlossen werden. Was sagt der Chatbot selbst dazu? «Es freut mich, dass die Vorabkontrolle für meinen Einsatz schnell abgeschlossen wurde. Allerdings möchte ich darauf hinweisen, dass ich primär hier bin, um Fragen rund um das Strassenverkehrs- und Schifffahrtsamt des Kantons Bern (SVSA) zu beantworten.»

Aus «VacMe» entsteht «HEMED»

«VacMe» hat eine Blitzkarriere hingelegt. Inmitten der Covid-19-Krise wurde die Anwendung entwickelt, geprüft und für die kantonale Impfkampagne eingesetzt. Zusammen mit der Pandemie endete auch die «Laufbahn» der Anwendung. Seit Anfang 2025 wird sie nicht mehr aktiv betrieben, sondern nur noch offline als Backup-Lösung für künftige Pandemien aufrechterhalten – ohne Personendaten. Die Gesundheitsdirektion (GSI) erkannte jedoch mehr Potenzial in dieser einheimischen IT-Lösung, die sie in Auftrag gegeben und mit der sie nun bereits einige Erfahrung gesammelt hatte.

Basierend auf der Grundinfrastruktur von «VacMe» liess die GSI eine Plattform für verschiedene medizinische Dienste entwickeln: die «HealthCare Engagement and Management Platform (HEMED)». Nebst der bereits bekannten Backup-Anwendung «VacMe» sollen darüber auch andere Anwendungen zur Bekämpfung von Infektionskrankheiten sowie zur Organisation und Abwicklung der schulärztlichen Untersuchungen laufen. Ausserdem soll es eine Schnittstelle zum elektronischen Gesundheitsdossier geben.

Weil «HEMED» das technische Fundament für die Einzelanwendungen bildet, wird es von der DSA gesondert geprüft. Das macht die Vorabkontrolle in zweierlei Hinsicht speziell: Erstens müssen wir mit der GSI abgleichen, welche Funktionen und Parameter «HEMED» mit den Anwendungen gemeinsam hat, damit bei den Vorabkontrollen der Anwendungen später keine Doppelspurigkeiten entstehen. Allein dieser Abgleich ist äusserst aufwendig, da mehrere Fachstellen involviert und die Anwendungen noch nicht vollständig entwickelt sind. Zweitens stellt «HEMED» eine technische Infrastruktur ohne Gesundheitsdatenverarbeitung dar. Somit ist auch unsere Vorabkontrolle vorwiegend technischer Natur. Sprich: Wir prüfen, ob «HEMED» die Grundvoraussetzungen zum Schutz sensibler Personendaten erfüllt, die dereinst in den Fachanwendungen bearbeitet werden. Die Anwendungen selbst werden in separaten Vorabkontrollen untersucht, die sich dann vermehrt den rechtlichen Fragen widmen: Welche Daten dürfen auf welcher Grundlage bearbeitet werden? Wie sind die Zugriffsberechtigungen organisiert? Wer trägt die Hauptverantwortung?

Aufgrund seiner Vielschichtigkeit dürfte uns das Projekt noch eine Weile beschäftigen. Den ersten Prüfdurchlauf der ISDS-Unterlagen für «HEMED» konnten wir kurz vor dem Jahreswechsel 2025/2026 abschliessen.

Grünes Licht für Zivilstands-Software

Von der Geburt über die Eheschliessung bis zum Tod – alle Bernerinnen und Berner haben im Laufe ihres Lebens mindestens einmal mit einem der sieben Zivilstandsämter des Kantons zu tun. Und sie alle landen früher oder später in deren Fachapplikation «PendenZA». In diesem Programm werden sämtliche noch hängigen Verfahren erfasst und bearbeitet, bis sie abgeschlossen sind, sprich: bis ein Kind rechtmässig adoptiert ist oder ein Mensch offiziell seinen neuen Namen trägt. «PendenZA» hilft unter anderem bei der Terminverwaltung und erstellt Statistiken. So lässt sich beispielsweise herausfinden, in welcher Lokalität besonders viele Zeremonien durchgeführt werden oder wie hoch der Ausländeranteil in Ehevorbereitungsverfahren ist. Weil die Software einerseits veraltet ist und andererseits nicht vollumfänglich den Anforderungen einer digitalen Verwaltung genügt, soll sie durch eine Nachfolgerin ersetzt werden: «PendenZA 2.0». Diese Anwendung verspricht auch einen Zusatznutzen für die Bevölkerung: Künftig sollen Termin- und Raumreservationen sowie deren Zahlung online möglich sein.

Da es sich um neue Software mit neuen Bearbeitungen teils sensibler Daten handelt, war «Pendenza 2.0» vorabkontrollpflichtig. Im Januar 2025 reichte das Amt für Bevölkerungsdienste (ABEV) die entsprechenden Unterlagen bei uns ein – und ein gutes halbes Jahr später konnten wir grünes Licht geben.

Zuvor haben wir uns jedoch eingehend mit dem Vorhaben beschäftigt und an zwei Stellen besonders nachgehakt. Zum einen fiel uns eine Schwachstelle bei der Verschlüsselung sensibler Daten auf: Die Dokumente werden zwar verschlüsselt gespeichert, erscheinen in den sogenannten Logfiles (Änderungsprotokollen) aber unverschlüsselt. Zum anderen stellte sich eine organisatorische Frage: Warum brauchen sämtliche Mitarbeitenden aller sieben Zivilstandsämter Zugriff auf alle «PendenZA»-Geschäfte – also auch auf die aus Nachbarregionen? Die Antwort des ABEV erschien uns plausibel: Zur Vermeidung von Mehrfachbuchungen (etwa durch Paare, die unbedingt an einem bestimmten Termin heiraten wollen) oder Betrugsversuchen (z. B. Scheinehe) prüfen die Mitarbeitenden, ob in anderen Zivilstandsämtern Verfahren hängig oder abgewiesen worden sind. Zudem landen die «PendenZA»-Fälle anschliessend ohnehin im schweizweiten Personenstandsregister, auf das alle Zivilstandsämter der Schweiz zugreifen können – und deren Angestellte wiederum unterliegen der Verschwiegenheitspflicht.

Für die DSA war die Angelegenheit damit erledigt: Erstens konnten die Behörden ihr Vorgehen nachvollziehbar begründen und auf eine Rechtsgrundlage verweisen (Zivilgesetzbuch). Zweitens sind die Risiken gering, weil in «PendenZA» kaum sensible Personendaten bearbeitet und nach drei Jahren ohnehin alle Inhalte gelöscht werden. Vor diesem Hintergrund wäre eine innerkantonale Zugriffsbeschränkung unverhältnismässig gewesen. Ähnlich entschieden wir hinsichtlich der unverschlüsselten Logfiles. Das ABEV sicherte uns zwar zu, mit dem Softwareanbieter nach einer Lösung zu suchen. Obwohl diese aber zum

Zeitpunkt des Vorabkontrollverfahrens noch nicht in Sicht war, stellten wir nach gründlicher Risiken-Nutzen-Abwägung einen positiven Bericht aus.

Langer Prozess, negativer Abschluss – und nun doch der Schlüssel zu einer Lösung?

Clouds sind ungemein praktisch. Im Gegensatz zur stationären Festplatte bieten sie grenzenlos Platz – und Sicherheit: Denn selbst wenn der PC vom Blitz getroffen wird oder das Firmengebäude brennt, bleiben die Daten unbeschadet in den «Wolken» und können von überall auf dem Globus abgerufen werden. Im grössten Vorteil der Cloud liegt allerdings auch ihr grösster Nachteil: Sobald man sie nutzt, gibt man Daten aus der Hand. Sie werden auf fremden Servern gespeichert. Und je globaler der Cloud-Anbieter agiert, desto ungewisser ist es, wo die Daten lagern, wo sie bearbeitet werden und wer alles Zugriff darauf hat. Der Begriff «Cloud» passt deshalb in doppelter Hinsicht: Was hinter einer Wolke passiert, sieht niemand.

Trotzdem setzen nebst Privatpersonen auch immer mehr Behörden auf die cloudbasierten Dienste grosser US-Konzerne wie Microsoft oder Google – und spätestens beim Bearbeiten sensibler Personendaten geht damit ein Risiko einher. Die genannten Firmen bieten bislang keine überzeugende Lösung für den Umgang mit vertraulichen und besonders schützenswerten Daten. Auch wenn diese verschlüsselt werden, sind sie vor Fremdzugriff nicht gefeit. Erstens behalten die Anbieter selbst den Hauptschlüssel. Zweitens kann sie der sogenannte *Cloud Act* zwingen, Kundendaten an US-Behörden auszuhändigen. Kurzum: Die Schweizer Behörden haben keine hinreichende Kontrolle darüber, wer auf ihre Daten zugreift.

Eine KDSG-konforme Bearbeitung sensibler Daten ist deshalb – Stand heute – mit Cloud-Dienstanbietern wie z. B. Microsoft und Google nicht möglich. Die Risiken für die betroffenen Personen sind zu hoch.

Darauf weist die DSA jede Behörde hin, die ein cloudbasiertes System solcher Anbieter implementieren will. Sensible Daten dürfen nur in der Cloud bearbeitet werden, wenn sie verschlüsselt sind und wenn allein die Behörde über den Schlüssel verfügt.

Ein Amt aus dem Bildungssektor liess sich davon nicht beirren. In der festen Überzeugung, die Risiken beseitigen zu können, legte es uns sein Projekt zur Vorabkontrolle vor. Elf Monate und etliche Mailwechsel später kam die DSA zum gleichen Ergebnis wie vor der Kontrolle. Von den ursprünglichen 58 Befunden konnten zwar einige behoben werden, das Kernproblem aber blieb bestehen: der drohende Kontrollverlust gegenüber dem Cloud-Anbieter aufgrund einer ungenügenden Verschlüsselungslösung. Im Juni 2025 stellten wir schliesslich einen negativen Abschlussbericht aus – für beide Seiten ein unbefriedigender Ausgang, denn beide hatten viel Zeit und Energie investiert.

Möglicherweise ist das letzte Wort aber noch nicht gesprochen. Ein DSA-Informatiker recherchierte akribisch im Angebotsportfolio des Softwarekonzerns, um doch noch fündig zu werden: Es gibt tatsächlich eine «Hold Your Own Key» (HYOK)-Lösung, bei welcher der Schlüssel zum Entschlüsseln der Daten allein beim Kunden bleibt. Selbst während der Bearbeitung – also im Austausch zwischen Prozessor und Arbeitsspeicher – bleiben die Daten verschlüsselt. Dies ist allerdings die einzige HYOK-Lösung des Konzerns und mit erheblichen Komplikationen verbunden. Die DSA wird prüfen, ob dies gleichwohl ein gangbarer Weg für die Bildungsbehörde und andere öffentliche Institutionen wäre.

6.5 Audits

Die DSA wird nicht nur *vor* der Einführung neuer Datenbearbeitungen aktiv, sondern oft auch hinterher. Die Überprüfung bereits in Betrieb stehender ICT-Systeme gehört ebenso zu ihrem gesetzlichen Auftrag wie Vorabkontrollen oder Beratungen. Allerdings können die Vor-Ort-Audits schon aus personellen Gründen nicht im gleichen Umfang erfolgen. Der zuständige Mitarbeiter (bislang einer) wählt die zu prüfenden Behörden nach bestimmten Kriterien aus (v. a. risikoorientiert) und führt jährlich – teils selbst und teils mit externer Unterstützung – bis zu zehn Audits durch.

Von den im Berichtsjahr geplanten acht Audits konnten nur zwei abgeschlossen werden. Zu vier Audits sind die Prüfungshandlungen erfolgt, der Abschluss (Abschlussbesprechung mit der geprüften Stelle und Finalisierung des Auditberichts) erfolgt aber erst Anfang 2026; über sie wird im Folgejahr berichtet. Die Prüfung des ICT-Grundschutzes eines Spitals wurde verschoben, weil sich dieses in einer betrieblichen Transformation befindet. Auf ein Audit musste aus personellen Gründen verzichtet werden.

Ein erfreulicher Kulturwandel

Theorie und Praxis sind zwei verschiedene Paar Schuhe: das eine existiert nur virtuell, mit dem anderen kann man loslaufen. All die Empfehlungen, die die DSA bei Behördenberatungen und Vorabkontrollen ausspricht, sollten nach Möglichkeit umgesetzt werden. Ob das geschieht, prüfen wir jedes Jahr bei ausgewählten Behörden vor Ort. Unsere Audits führen wir entweder allein oder gemeinsam mit einem Partner durch. Dabei müssen wir leider immer wieder feststellen: Die gesetzlichen Ansprüche in puncto Informationssicherheit und Datenschutz (ISDS) kollidieren vielerorts mit einer von Personalmangel, knappen Budgets und Zeitdruck geprägten Wirklichkeit. Wer schon im Kerngeschäft an seine Grenzen kommt, misst dem Datenschutz weniger Priorität bei. Vielen Institutionen mangelt es an einem ganzheitlichen Blick auf ISDS, es fehlen klare

Konzepte und Rollenzuweisungen. Die zuständigen Mitarbeitenden haben selten ein Sprachrohr auf Führungsebene.

Doch die Zeiten ändern sich. Seit einigen Jahren vollzieht sich ein Kulturwandel, den wir auch in den von uns geprüften Behörden feststellen. Das Bewusstsein für die elementare Bedeutung von Informationssicherheit und Datenschutz wächst, Mitarbeitende bekennen sich zu und identifizieren sich mit dem Thema. Besonders deutlich zeigte sich dies in den 2025 auditierten Spitälern. Nie zuvor habe er in den 20 Jahren seiner Anstellung eine solche ISDS-Qualität erlebt, so das Feedback eines Spitalmitarbeiters.

Ein vergleichbares Commitment konnten wir in der Pädagogischen Hochschule (PH) Bern beobachten.

PHBern – auf dem richtigen Weg, noch nicht am Ziel

Während unserer Prüfung zeigte sich die PHBern überaus kooperativ und aufrichtig. Die Bildungs- und Forschungseinrichtung geht das Thema ISDS systematisch an und ist dabei, es in verlässliche Strukturen zu überführen. Davon, dass der Kulturwandel dort angekommen ist, zeugte auch die Anwesenheit eines Geschäftsleitungsmitglieds.

Allerdings befinden sich besagte Strukturen noch im Aufbau. In den neun von uns geprüften Bereichen – von der ISDS-Governance bis hin zur physischen Sicherheit – mussten wir 23 Befunde ausstellen. Ohne klare Rollenzuweisungen für IT-Systeme besteht beispielsweise die Gefahr, dass sich niemand für die Umsetzung von Informationssicherheit und Datenschutz verantwortlich fühlt. Und wenn Zugriffsrechte nicht eindeutig geregelt sind, können die falschen Personen mitunter zu viele Einblicke bekommen.

Um sich gegen immer professioneller werdende Cyberangriffe verteidigen zu können, muss man systematisch Sicherheitschecks und Penetrationstests durchführen – auch daran mangelt es bei der PH bisher. Nebst diesen organisatorischen Defiziten besteht auch ein physisches, was den Standort der Server betrifft.

Diese Beispiele zeigen: Die PH hat sich zwar auf einen guten Weg gemacht, ist aber noch nicht am Ziel. Eine schnellere Umsetzung geben die Ressourcen der Hochschule zurzeit nicht her, doch ihre Haltung scheint zu stimmen. Die Verantwortlichen fühlen sich der Datensicherheit verpflichtet und bekennen sich zum Abschlussbericht des Audits.

6.6 Weitere aufsichtsrechtliche Instrumente

6.6.1 Gemeldete Datenschutzvorfälle

Auch bei noch so sicherer IT-Infrastruktur kann es passieren, dass Daten verloren gehen oder in die falschen Hände geraten – sei es durch Unaufmerksamkeit, Unwissenheit oder Fahrlässigkeit. Wichtig ist, dass derlei Datenschutzvorfälle erkannt, Schäden möglichst verhindert und Wiederholungen durch präventive Massnahmen künftig vermieden werden. Eine Meldung an die DSA ist bislang nur bei Vorfällen im Bereich Polizeiarbeit und Strafvollzug erforderlich. Mit der Totalrevision des KDSG wird diese Pflicht auf alle öffentlichen Aufgaben ausgedehnt. Bereits heute empfehlen wir aber sämtlichen Behörden, uns ihre Datenschutzvorfälle zu melden, damit wir gemeinsam allfällige Massnahmen koordinieren können. Jedes Jahr nehmen einige Behörden dieses Angebot wahr – womit sie eine gesunde Fehlerkultur und ein ausgeprägtes Bewusstsein für Datenschutz beweisen.

Im Berichtsjahr wurden uns neun Vorfälle gemeldet; darunter ein erfolgreicher Phishing-Angriff, eine zu informative Excel-Tabelle, im Zug vergessene Dokumente und ein E-Mail-Empfänger, der versehentlich ins CC geraten war. In zwei Fällen kam es zu einem unsachgemässen Gebrauch des KI-Bots «ChatGPT». Einen davon schildern wir im Folgenden ausführlicher, weil er eine gewisse mediale Aufmerksamkeit erhielt und weil uns das Thema KI in Zukunft häufiger beschäftigen dürfte.

«ChatGPT»: Risikofaktor Mensch

«Wann und wie soll ich meine Orchideen zurückschneiden?» «Werte meine MRI-Bilder aus!» «Schreib mir eine Gute-Nacht-Geschichte, in der mein Enkel vorkommt!» Ob als Alltagsratgeber, Ersatzärzte oder Textgehilfen – KI-Bots unterstützen uns mittlerweile in jeder Lebenslage. Was den wenigsten von uns bewusst ist: Die Daten, mit denen wir sie füttern, bleiben nicht bei uns. Sie landen auf unbekannten Servern und werden – sofern wir diese Funktion nicht deaktivieren – zu Trainingszwecken weiterverwendet. Mit etwas Pech sind unsere scheinbar privaten KI-Chats dann via Google-Suche auffindbar (so geschehen im Juli 2025, wie diverse Medienberichte offenbarten). Wir sind also gut beraten, keine vertraulichen Informationen mit dem Bot zu teilen. Das gilt insbesondere für öffentliche Institutionen wie die Berner Fachhochschule (BFH). Diese ist letztes Jahr wegen unsachgemässen Umgangs mit «ChatGPT» in die Schlagzeilen geraten und war auch Gegenstand einer DSA-Untersuchung. Eine Angestellte hatte mithilfe des KI-Tools ein Arbeitszeugnis für ihren Mitarbeiter erstellen lassen und dazu allerlei Daten des Betroffenen eingespeist: Klarnamen,

Geburtsdatum, Adresse, Abschlüsse etc. Dieses Vorgehen war nicht nur aus oben genannten Gründen heikel, sondern auch, weil sich mehrere Mitarbeitende einen privaten «ChatGPT»-Account teilten. Nebst unbekannten Dritten hatten also auch Kolleginnen und Kollegen des Betroffenen Zugriff auf dessen Daten.

Nachdem uns dieser Vorfall gemeldet worden war, kontaktierten wir die Hochschule, um die Vorwürfe des Betroffenen zu verifizieren und um zu erfahren, welche Konsequenzen die BFH daraus zieht. Deren Datenschutzbeauftragte präsentierte uns eine Reihe präventiver und personalrechtlicher Massnahmen – von Schulungs- und Informationsangeboten über eine Aussprache mit dem Betroffenen bis hin zur Verwarnung der beteiligten Mitarbeitenden. Aus unserer Sicht ist das Massnahmenpaket angemessen und dazu geeignet, weitere Vorfälle dieser Art möglichst zu verhindern.

Die Weitergabe personenbezogener Daten durch öffentliche Behörden ist schliesslich keine Bagatelle, sondern eine Rechtsverletzung. Und wenn wie im Falle von «ChatGPT» keine technischen Schutzmassnahmen möglich sind, so muss wenigstens der Risikofaktor Mensch minimiert werden: durch klare Rollenzuteilungen, Arbeitsinstruktionen und letztlich auch durch Sanktionen.

6.6.2 Prüfung der automatisierten Fahrzeugfahndung

Seit August 2024 enthält das kantonale Polizeigesetz ausführliche Vorschriften über die automatisierte Erfassung von Fahrzeugkontrollschildern und deren Abgleich mit polizeilichen Datenbanken. Auch wenn dieser Abgleich keine Übereinstimmung ergibt, können die Daten bis zu 60 Tage aufbewahrt und unter bestimmten Voraussetzungen später erneut ausgewertet werden. Im Gesetzgebungsverfahren hatten wir diese umfangreiche Vorratsdatenhaltung kritisiert (s. Jahresbericht 2022, Ziff. 6.2), beim Grossen Rat aber kein Gehör gefunden. Stattdessen legte dieser fest, dass wir regelmässig die Einhaltung der gesetzlichen Vorschriften kontrollieren und unsere Feststellungen jeweils veröffentlichen. Dazu können wir uns einerseits auf den Bericht stützen, den die Datenschutzverantwortliche der KAPO regelmässig erstellen muss. Andererseits können wir aber auch eigene Prüfungen durchführen. Zudem muss die KAPO jährlich einen allgemein zugänglichen Bericht über die Wirksamkeit der automatisierten Fahrzeugfahndung veröffentlichen.

Weil eine Beschwerde Dritter beim Bundesgericht hängig war, verzichtete die KAPO im Berichtsjahr auf die Aufbewahrung der o. g. Daten. Wir beschränkten unsere Kontrolle mithin auf den uns vorgelegten Bericht der Datenschutzverantwortlichen. Demzufolge generierten die 46 stationären Geräte monatlich bis zu 796 Treffer im automatisierten Abgleich. Zusammen mit den Treffern der 9 mobilen Geräte wurden zwischen Januar und Juli 2025 insgesamt 51.757 Treffer erzielt, die zu rund 150 Anhaltungen betreffend verschiedene Deliktkategorien

führten. Aus dem Bericht ergeben sich keine Anhaltspunkte, wonach die gesetzlichen Vorschriften nicht eingehalten worden wären.

6.6.3 Begründete Anträge und Beschwerdeverfahren

Stellen wir Verstösse gegen das Datenschutzrecht oder Mängel bei der Datensicherheit fest, so können wir deren Beseitigung in Form eines begründeten Antrags empfehlen. Will die verantwortliche Behörde unserem Antrag nicht oder nur teilweise stattgeben, so erlässt sie eine Verfügung, die wir bei der zuständigen Direktion bzw. beim Verwaltungsgericht anfechten können. In der Praxis sprechen wir unsere Empfehlungen – namentlich nach aufsichtsrechtlichen Rückfragen, bei Vorabkontrollen und Audits – nicht als formelle Anträge in diesem Sinne aus, weil die Behörden fachlich nachvollziehbare Empfehlungen meist von sich aus umzusetzen bereit sind. Erst wenn eine Behörde ein wichtiges Anliegen der DSA (wie die Beseitigung einer klaren Rechtsverletzung oder eines hohen Risikos) nicht befolgen würde, müssten wir den formellen Weg beschreiten.

Im Berichtsjahr erliessen wir keinen formellen Antrag und führten keine Beschwerde gegen die ablehnende Verfügung einer verantwortlichen Behörde.

6.6.4 Oberaufsicht über die kommunalen Aufsichtsstellen

Nach dem heutigen KDSG haben alle Gemeinden und anderen gemeinderechtlichen Körperschaften sowie die Landeskirchen eigene Datenschutzaufsichtsstellen; die DSA übt die Oberaufsicht aus und ist Anlaufstelle für die kommunalen Aufsichtsstellen.

Verschiedene von ihnen – oft sind es die Rechnungsprüfungsorgane der Gemeinden – gelangten mit Fragen an die DSA, weil sie selbst unsicher waren. In den meisten Fällen ging es um die Bekanntgabe von Personendaten durch eine Gemeindebehörde an Dritte, etwa wenn Betroffene eine Datensperre veranlasst hatten. Wir erklärten den Aufsichtsstellen jeweils, dass Datensperren nur gegenüber privaten Dritten und nicht gegenüber anderen Behörden wirksam sind. Den gesetzlich vorgesehenen Informationsaustausch unter Behörden können die Bürgerinnen und Bürger nicht auf diese Weise verhindern.

Viele Anfragen kamen auch von Gemeindebehörden selbst, weil sie entweder gar nicht wussten, dass sie eine eigene Aufsichtsstelle haben, oder weil diese ihnen nicht weiterhelfen konnte. In den Fragen ging es zumeist ebenfalls um Datenbekanntgaben bei einer Sperrung, aber auch um Videoüberwachungen oder um den Einsatz neuer Technologien wie Cloud-Services und KI.

6.7 Sensibilisierung/Aufklärung

Mitwirkung bei der Ausbildung von Gemeindepersonal

Das Bildungszentrum für Wirtschaft und Dienstleistung (bwd) bietet verschiedene Lehrgänge und Kurse für Gemeindepersonal an, in deren Rahmen DSA-Mitarbeitende seit vielen Jahren das Fach «Datenschutz und Informationssicherheit» unterrichten. Im Berichtsjahr fanden ein Lehrgang zur Erlangung des Fachausweises Bernische Gemeindefachfrau/Bernischer Gemeindefachmann, ein Lehrgang für Mitarbeitende der Schuladministration und ein Kurs zum Datenschutz in Kirchgemeinden statt. An den Weiterbildungen erläuterten wir die Grundsätze des Datenschutzrechts anhand konkreter Beispiele aus den Fachbereichen der Kursteilnehmenden. Diese konnten (und sollten) Fragen aus ihrem Arbeitsalltag stellen, die dann im Plenum diskutiert und beantwortet wurden.

Ferner wurde der Datenschutzbeauftragte zur Jahresversammlung der Gemeindeschreiberinnen und Gemeindeschreiber der Region Bern eingeladen, um über die Themen Datenschutz und KDSG-Revision zu berichten.

Wissensvermittlung im Rahmen spezifischer Anlässe

Auf Anfrage referieren Vertreterinnen und Vertreter der DSA an Fach- und Weiterbildungsanlässen. Im Berichtsjahr sprachen sie über «Datenschutz und Sprachtechnologie» am Weiterbildungsseminar der Sprachdienste der Kantonsverwaltung, über «M365 im Kanton Bern» an einer Veranstaltung des Datenschutz-Forums Schweiz und über «Datenschutz kompakt» an einer internen Weiterbildung des Amts für Integration und Soziales.

News und Infos auf der DSA-Website

Ihre Website hat die DSA bislang eher sporadisch bespielt. Das soll sich ändern: Die Themen Datenschutz und Informationssicherheit sind zu wichtig, als dass sie ein Schattendasein fristen sollten. Nicht nur im Hinblick auf die KDSG-Revision wollen wir unsere kommunikativen Tätigkeiten ausbauen, sondern auch zur Sensibilisierung der Öffentlichkeit. Seit Herbst 2025 machen wir deshalb vom kantonalen News-Service Gebrauch. Regelmässig berichten wir aus unserem Arbeitsalltag: Wir erläutern unsere Stellungnahmen zu gewissen Gesetzesvorhaben, vermelden Neuigkeiten, die uns direkt betreffen, und illustrieren die Vielfalt des Datenschutzthemas mithilfe ausgewählter Beispiele (Rubrik «Aus dem Alltag»). Dabei setzen wir auf eine Sprache, die weitgehend ohne Paragrafen auskommt und auch Interessierte ohne grosses Vorwissen abholt. Die News sind auf unserer Website abonnierbar und landen auf Wunsch automatisiert im Mail-Postfach.

Darüber hinaus soll die DSA-Website auch für kommunale Behörden zur informativen Anlaufstelle werden. Entsprechende Hilfsmaterialien wollen wir möglichst bedürfnisorientiert erstellen, weswegen wir die Bedürfnisse der Gemeinden bereits im Vorfeld der KDSG-Revision einholen. Zu diesem Zweck haben wir uns bisher u. a. mit dem Verband Bernischer Gemeinden, zwei Regierungsstatthalterinnen und dem AGR ausgetauscht sowie an einem Gemeindeschreibertreffen teilgenommen.

6.8 Interkantonale Zusammenarbeit

Präsidium und Vorstand von privatim

Seit Ende 2020 präsidiert DSA-Leiter Ueli Buri die Konferenz der schweizerischen Datenschutzbeauftragten, privatim. In diesem Verbund sind alle kantonalen und einige kommunale Datenschutzbehörden, der EDÖB als beratendes Mitglied sowie die Datenschutzbeauftragte des Fürstentums Liechtenstein als Beobachterin vereint, um den Anliegen des Datenschutzes Gehör zu verschaffen und die Zusammenarbeit unter den Datenschutzbehörden zu fördern. Im Berichtsjahr führte privatim zwei Plenumsversammlungen durch und befasste sich schwergewichtig mit der Bearbeitung von Gesundheits- und anderen sensiblen Daten in Cloud-Services. Eine im November verabschiedete Resolution, wonach solche Daten nicht in «Software-as-a-Service»(SaaS)-Lösungen internationaler Anbieter – z. B. «M365» – bearbeitet werden dürfen, stiess auf grosses Interesse in Schweizer Fach- und allgemeinen Medien. Auch in Deutschland blieb die Resolution nicht unbemerkt.

Privatim verfasste 13 Stellungnahmen im Rahmen von Vernehmlassungen des Bundes oder der Regierungs- bzw. Direktorenkonferenzen. Die Stellungnahmen dienten den privatim-Mitgliedern z. T. als Vorlage für Eingaben in ihren jeweiligen Kantonen. In zahlreichen Kontakten mit interkantonal tätigen Organisationen – namentlich der Digitalen Verwaltung Schweiz, der Fachagentur Educa, der Schweizerischen Berufsbildungsämter-Konferenz, der Körperschaft für Polizeitechnologie und Informatik (PTI) sowie der Schweizerischen Archivdirektorinnen- und Archivdirektorenkonferenz – beriet privatim zu Fragen des Datenschutzes und der Informationssicherheit. Im regelmässig stattfindenden Austausch mit dem EDÖB wurden Fragen zu fachlichen Details oder zur Abgrenzung der jeweiligen Aufsichtszuständigkeiten diskutiert und geklärt.

Arbeitsgruppen von privatim

Die *Arbeitsgruppe Digitale Verwaltung* arbeitete im Berichtsjahr an einem Merkblatt über die datenschutzkonforme Nutzung webbasierter Dienste, die mithilfe künstlicher Intelligenz Texte, Bilder, Videos, Musik oder Codes erzeugen. Das Merkblatt soll sich an die Verantwortlichen innerhalb von Kantons- und Gemeindeverwaltungen richten und diesen die Datenschutzrisiken sowie mögliche Massnahmen dagegen aufzeigen.

Die von der stellvertretenden Datenschutzbeauftragten Rahel Lutz geleitete *Arbeitsgruppe Gesundheit* befasste sich unter anderem mit der Überschneidung der Aufsichtskompetenzen der kantonalen Datenschutzbehörden und des EDÖB in privatrechtlich organisierten Spitälern mit einem staatlichen Versorgungsauftrag (s. dazu auch Ziffer 3: «Mehrere Ebenen im selben Unternehmen»). Ausserdem erfolgte ein Wissens- und Erfahrungsaustausch zu zahlreichen weiteren aktuellen Fragestellungen, die mehrere oder alle Mitglieder von privatim betreffen.

Die *Arbeitsgruppe Sicherheit* begleitete weiterhin das Projekt des Bundes und der Kantone zur Errichtung einer übergreifenden Abfrageplattform für Polizeidaten (POLAP). Dafür sind neue Rechtsgrundlagen zu schaffen, wobei die Kantone ihre Rechte und Pflichten richtigerweise in einem Konkordat vereinbaren. Offenbar gibt es Kantone, die ihr kantonales Polizeigesetz ergänzen und keinem Konkordat beitreten wollen. Dass dies rechtlich und praktisch zu Schwierigkeiten führen dürfte, erkannte auch das Bundesgericht in einem Entscheid zum Polizeigesetz des Kantons Luzern.

In der *Arbeitsgruppe ICT* besprachen Spezialistinnen und Spezialisten für Informations- und Cybersicherheit jener Aufsichtsstellen, die über solche verfügen, aktuelle technische Fragen und Entwicklungen.

7 Fünf-Jahres-Übersicht: der DSA-Alltag in Zahlen

Die in Kapitel 6 servierten «Kostproben» sollen zur Veranschaulichung unseres Arbeitsalltags dienen: Auf welche Details achten wir in Vorabkontrollen, welche Art von Anfragen erreichen uns, wie finden wir die Mitte zwischen zu strenger Kontrolle und zu grosser Kulanz?

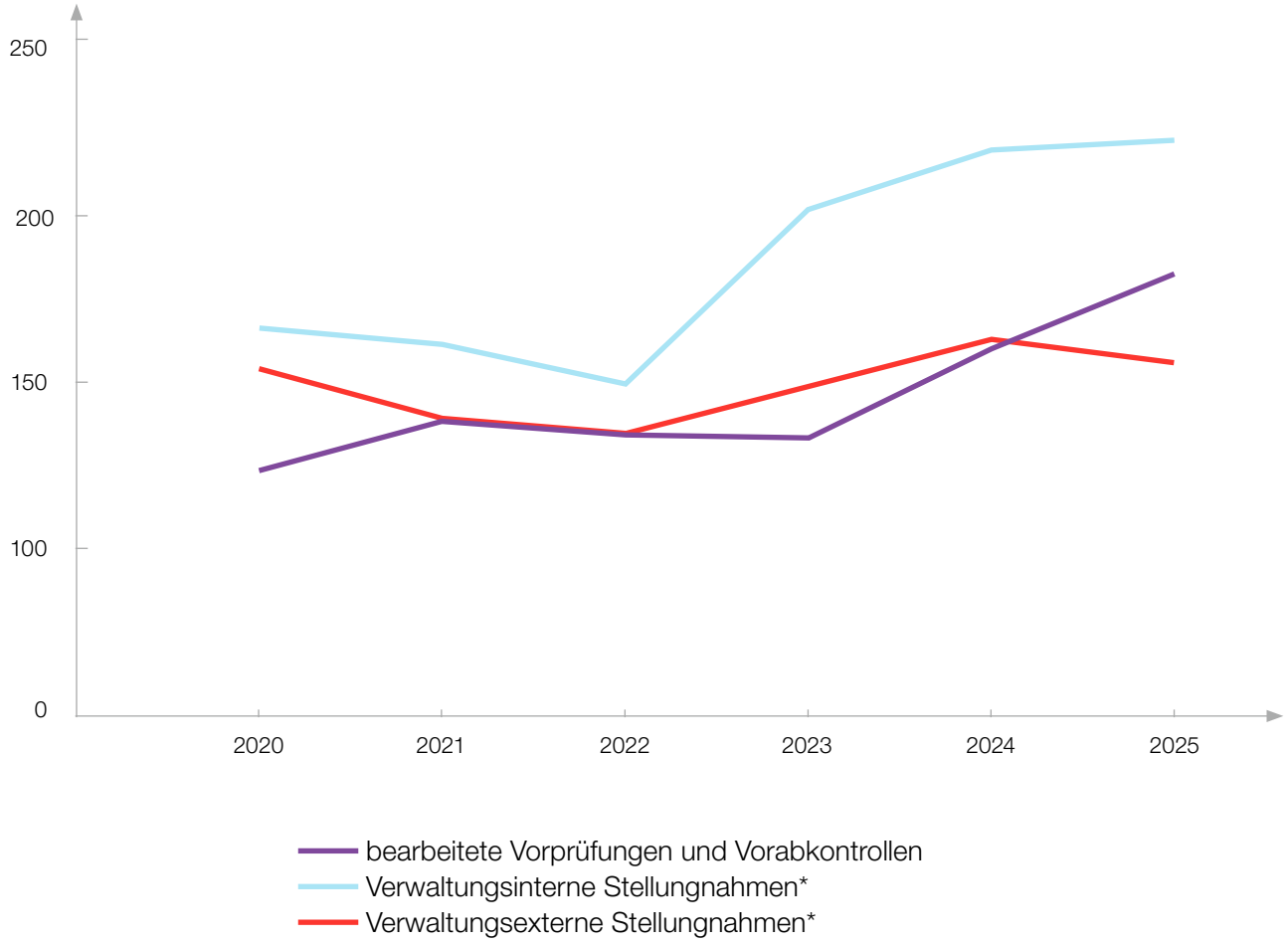
Was bis hierhin noch fehlt, sind Zahlen.

Die folgende Tabelle zeigt, wie viele Geschäfte aus den Bereichen Vorabkontrollen, Audits sowie interne und externe Stellungnahmen wir in den letzten fünf Jahren bearbeitet haben. Dazu ein kleiner Lesehinweis: Bevor wir eine Vorabkontrolle starten, führen wir in der Regel eine Vorprüfung durch. Dabei entscheiden wir, ob ein Projekt überhaupt kontrollpflichtig ist und ob die bis dahin vorliegenden Unterlagen «kontrollreif» sind (d. h. den formalen Anforderungen genügen und hinreichend aussagekräftig sind). Zum Verständnis der Tabelle ist ausserdem wichtig: Nicht jede eröffnete Vorabkontrolle wird im selben Jahr abgeschlossen. Einige beschäftigen uns über mehrere Jahre, andere lassen sich bedeutend schneller erledigen. So kommt es, dass die Zahlen «eröffnete Geschäfte» und «abgeschlossene Geschäfte» nicht übereinstimmen und dass die «bearbeiteten Geschäfte» *nicht* als Gesamtsumme dieser beiden Einheiten zu verstehen sind.

	2020	2021	2022	2023	2024	2025
Vorprüfungen und Vorabkontrollen						
bearbeitete Geschäfte	123	138	134	133	160	183
neu eröffnete Geschäfte	74	78	69	83	86	88
abgeschlossene Geschäfte	58	77	94	63	90	95
Audits (inkl. Nachaudits)	7	9	12	9	8	2
Verwaltungsinterne Stellungnahmen*	166	161	149	202	220	223
davon informelle Beratungen	92	80	88	135	146	144
davon formelle Stellungnahmen	74	81	61	67	74	79
Verwaltungsexterne Stellungnahmen*	154	139	134	148	163	156
davon Private	114	98	90	94	105	113
davon Gemeindebehörden	40	41	44	54	58	43

* In der Geschäftsverwaltung neu eröffnete Geschäfte, ohne Folgearbeiten zu in Vorjahren eröffneten Geschäften, ohne Mehrfachäusserungen zum gleichen Geschäft und ohne telefonische Auskünfte.

Das folgende Liniendiagramm zeigt, wie sich die Anzahl der von aussen an uns gelangten Geschäfte in den letzten Jahren entwickelt hat (Audits planen wir selbst und werden deshalb nicht aufgeführt). Dabei lässt sich vor allem bei den verwaltungsinternen Stellungnahmen (z. B. Behördenberatung oder Mitberichte) eine steigende Tendenz ablesen. Auch die Vorabkontrollgeschäfte haben in den letzten zwei Jahren merklich zugenommen. Vor dem Hintergrund der KDSG-Revision rechnen wir mit einer weiteren Zunahme.



8 Antrag

Kenntnisnahme

9 Glossar / Abkürzungen

Abkürzung	Beschrieb
ABEV	Amt für Bevölkerungsdienste
ADC BEJUNE	Association pour le dépistage du cancer Berne, Jura et Neuchâtel
AGOV	**A**uthentifizierungsdienst **GOV**ernment (Login für Zugang zu Behördendiensten)
AGR	Amt für Gemeinden und Raumordnung
AHV	Alters- und Hinterlassenenversicherung
AKVB	Amt für Kindergarten, Volksschule und Beratung
BAZG	Bundesamt für Zoll und Grenzsicherheit
BFH	Berner Fachhochschule
BJ	Bundesamt für Justiz
BRAICS	Breast cancer-Related Approach for Increasing cervical Cancer Screening
bwd	Bildungszentrum für Wirtschaft und Dienstleistung
CC	Zusätzliche Empfängerzeile bei E-Mails (Carbon Copy)
ChatGPT	Chatbot Generative Pre-trained Transformer
DIJ	Direktion für Inneres und Justiz
DSA	Datenschutzaufsichtsstelle des Kantons Bern
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Educa	Schweizerische Fachagentur für den digitalen Bildungsraum
ESBK	Eidgenössische Spielbankenkommission
FAQ	Frequently Asked Questions (Sammlung oft gestellter Fragen und der Antworten darauf)
FIN	Finanzdirektion
GERES	Gemeinderegistersystem
GSI	Gesundheits-, Sozial- und Integrationsdirektion

HEMED	HealthCare Engagement and Management Platform
HYOK	Hold Your Own Key (Verschlüsslungsverfahren/Schlüsselselbstverwaltung)
ICE	Intercity-Express
ICT	Informations- und Telekommunikationstechnik
ISDS	Informationssicherheit und Datenschutz
I-SIVE	Informationssicherheitsverantwortliche/r
IT	Informatik
JVA	Justizvollzugsanstalt
KAIO	Amt für Informatik und Organisation
KAPO	Kantonspolizei
KDSG	(Kantonales) Datenschutzgesetz
KESB	Kindes- und Erwachsenenschutzbehörde(n)
KI	Künstliche Intelligenz
KUW	Kirchliche Unterweisung
M365	Microsoft 365
NFFS	Neues Fallführungssystem
PC	Personal Computer
PHBern	Pädagogische Hochschule Bern
POLAP	Nationale Abfrageplattform für Polizeidaten
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
PTI	Körperschaft Polizeitechnik und -informatik Schweiz
s.	siehe
SaaS	Software-as-a-Service
SAK	Grossrats-Kommission für Staatspolitik und Aussenbeziehungen

SMS	Short Message Service/Kurznachrichtendienst
SN2	Schutzniveau 2 (für besonders schützenswerte Personendaten oder vertrauliche Informationen)
STA	Staatskanzlei
SVSA	Strassenverkehrs- und Schifffahrtsamt
US(A)	Vereinigte Staaten (von Amerika)
WEU	Wirtschafts-, Energie- und Umweltdirektion
Ziff.	Ziffer

Datenschutzaufsichtsstelle
des Kantons Bern

Poststrasse 25
3072 Ostermundigen
+41 31 633 74 10
datenschutz@be.ch

www.be.ch/dsa