Kanton Bern
Canton de Berne

Jahresbericht Datenschutzaufsichtsstelle 2024

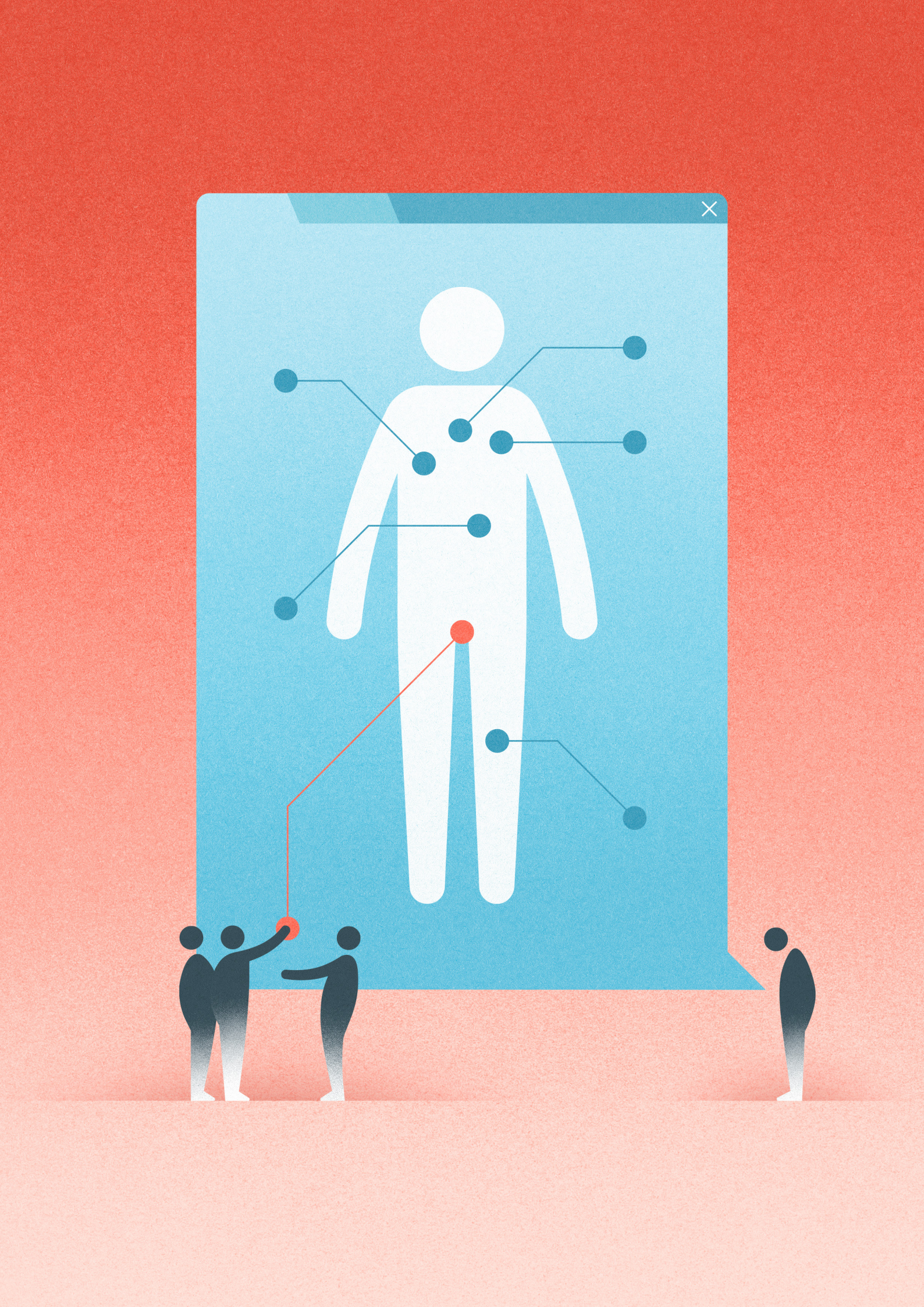
Datenschutzaufsichtsstelle

Februar 2025

Impressum

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

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



1 Vorwort

Das erste – heute noch gültige – Datenschutzgesetz des Kantons Bern von 1986 dient nach seinem Zweckartikel «dem Schutz von Personen vor missbräuchlicher Datenbearbeitung durch Behörden». An dieser Beschreibung positiv ist, dass schon damals nicht der Schutz der Daten als solche im Zentrum stand, sondern der Schutz der Personen, um deren Daten es geht. Als etwas bedenklicher erscheint es, dass offenbar davon ausgegangen wurde, dass die Behörden die Personendaten missbrauchen könnten und es ein besonderes Gesetz braucht, um dies zu verhindern. Diese Sichtweise ist heute überholt. Die Kantonsverfassung von 1993 enthält ein eigenständiges Grundrecht auf Datenschutz, dessen wesentlichsten Gehalte die Gesetzmässigkeit und Verhältnismässigkeit jeder behördlichen Datenbearbeitung, die Richtigkeit und Sicherheit der Daten sowie die Rechte der betroffenen Personen auf Einsicht in ihre Daten darstellen. Folgerichtig geht der vom Regierungsrat im November 2024 zuhanden des Grossen Rats verabschiedete Entwurf für ein neues Datenschutzgesetz von einer umfassenderen Zweckbestimmung aus: «Dieses Gesetz bezweckt den Schutz des Grundrechts auf Datenschutz von Personen, über die Behörden Personendaten bearbeiten».

Der Schutz der Privatsphäre ist kein absolutes Recht, sonst könnten die Behörden die ihnen aufgetragenen öffentlichen Aufgaben nicht erfüllen. Die im Grundrecht auf Datenschutz der Berner Kantonsverfassung enthaltenen rechtsstaatlichen Spielregeln sind jedoch nicht verhandelbar. Dies gilt auch bzw. erst recht für digitale Datenbearbeitungen, deren technische Möglichkeiten – das spielend leichte Kopieren, Verknüpfen und Übermitteln von Daten, das Aufbewahren ohne physischen Platzbedarf, das weltweite Angebot von fortschrittlichen Verarbeitungsvorgängen zu erschwinglichen Preisen – erhöhte Risiken für die Rechte der betroffenen Personen bringen. Bei jedem Vorhaben von Behörden, ihre Datenbearbeitungen auf den neusten technischen Stand zu bringen, stellt sich deshalb nie die Frage, ob die fachlichen Anforderungen oder die Anliegen des Datenschutzes und der Informationssicherheit Vorrang geniessen, sondern es muss stets ein «sowohl als auch» gelten.

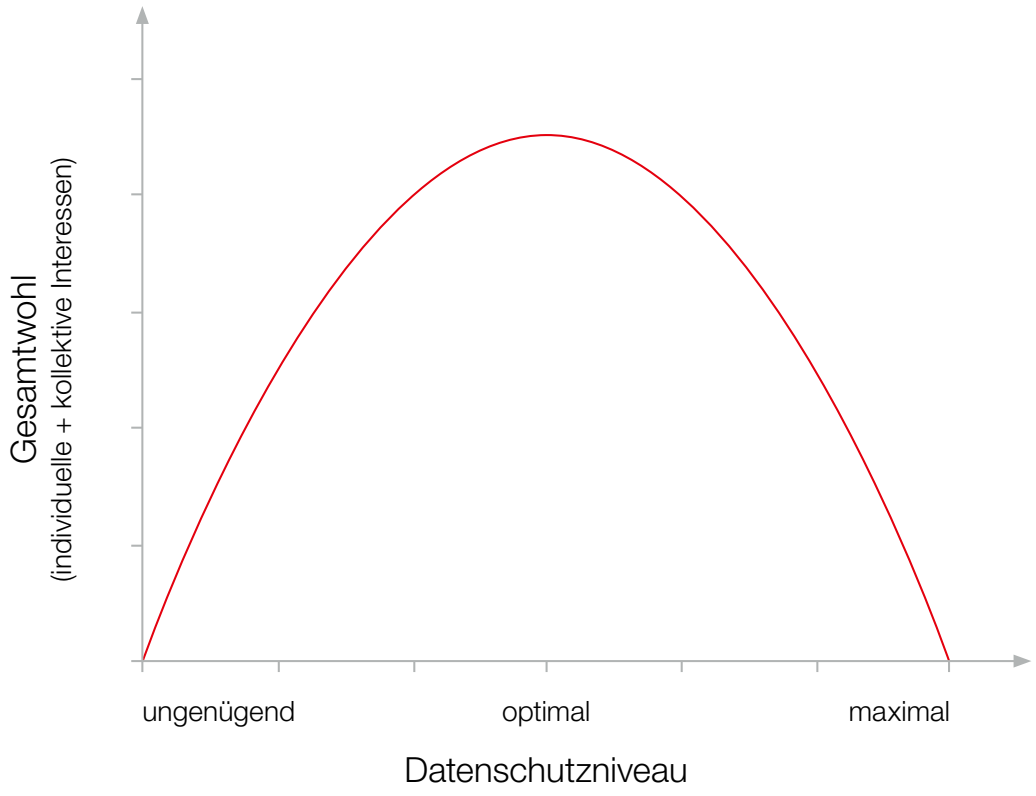
Die Datenschutzaufsichtsstelle des Kantons Bern (DSA) berät und beaufsichtigt die kantonalen Behörden bei deren Digitalisierungsprojekten. Je früher sie in ein Vorhaben einbezogen wird und die datenschutzrechtlichen Leitlinien aufzeigen kann, desto grösser ist der Spielraum der Behörden, das Projekt innerhalb dieser Leitlinien umzusetzen und alle Ziele unter Einhaltung der verfassungsrechtlichen Rahmenbedingungen zu erreichen. Im Jahr 2024 betreute die DSA erneut eine Vielzahl von Digitalisierungsvorhaben aus allen Verwaltungsbereichen. Über eine Auswahl davon und die übrige Tätigkeit der DSA wird vorliegend berichtet.

Ueli Buri, Datenschutzbeauftragter

2 Grundrecht auf Datenschutz

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 eines Grundrechts – 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 (d. h. geeignet, notwendig und für die betroffenen Personen zumutbar) sein. Zum Grundrecht auf Datenschutz gehört nach der Berner Verfassung auch, dass die bearbeiteten Daten richtig sein müssen und vor missbräuchlicher Verwendung zu schützen sind (Datensicherheit).

Auf der anderen Seite weist die Kantonsverfassung den Behörden von Kanton und Gemeinden öffentliche Aufgaben – etwa in den Bereichen Bildung, Gesundheit, Wirtschaft oder Sicherheit – zu, welche im Interesse der Gemeinschaft zu erfüllen sind. Jenes Interesse kann im Falle einer Kollision mit der Privatsphäre von Einzelpersonen überwiegen. Den von der Verfassung gewährleisteten Datenschutz verstehen wir deshalb als *angemessenen* Datenschutz, welcher den Schutz individueller Grundrechte einerseits sowie die Interessen der Gemeinschaft an der Erfüllung der öffentlichen Aufgaben und einer wirkungsvollen Verwaltungstätigkeit andererseits zum bestmöglichen Ausgleich bringt.



Das optimale Schutzniveau liegt beim höchsten Gesamtwohl aus der Verwirklichung von individuellen und kollektiven Interessen.

Das Datenschutzgesetz (KDSG) konkretisiert die Pflichten der Behörden beim Bearbeiten von Personendaten, wobei nebst der Verwaltung auch weitere Träger von öffentlichen Aufgaben, z. B. Schulen und Spitäler, als Behörden gelten. Das «Bearbeiten» umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten. Daten dürfen nur zu einem bestimmten Zweck beschafft und grundsätzlich nicht für andere Zwecke bearbeitet werden. Das Gesetz hält sodann die Rechte der betroffenen Personen fest, namentlich das Recht auf Auskunft und Einsicht in ihre Daten, auf Berichtigung falscher und Löschung nicht benötigter Angaben über sie. Schliesslich regelt es die Stellung und Aufgaben der kantonalen und kommunalen Aufsichtsstellen gegenüber den Behörden und betroffenen Personen.

3 Verantwortung und Aufsicht

Für den Datenschutz ist jene Behörde verantwortlich, welche die Personendaten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeitet oder von einem Dritten bearbeiten lässt. Sie muss dafür sorgen, dass die Vorschriften über den Datenschutz eingehalten werden und die Datensicherheit gewährleistet ist. Dies gilt unabhängig davon, ob die zuständige Aufsichtsstelle involviert wird oder nicht und ob Empfehlungen derselben befolgt werden.

Das schweizerische und bernische Datenschutzrecht ist föderalistisch aufgebaut: Für die Bundesbehörden und die privaten (insbes. gewerblichen) Datenbearbeiter gilt das Datenschutzgesetz des Bundes (DSG), und die Aufsicht obliegt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Für die kantonalen und kommunalen Behörden im Kanton Bern gilt das KDSG, wobei die Aufsicht noch einmal zweigeteilt ist: Die DSA beaufsichtigt die Datenbearbeitungen durch kantonale Behörden; die Gemeinden bezeichnen für ihren Bereich eine eigene Aufsichtsstelle, über die die DSA die Oberaufsicht ausübt.

Im Einzelfall kann die Ermittlung des anwendbaren Rechts und der zuständigen Aufsichtsbehörde eine vertiefte Prüfung erfordern: So untersteht die privatrechtliche Stiftung «Swisstransplant» zuerst einmal – etwa bei der Bearbeitung der Daten ihres Personals – den Vorschriften des DSG für private Datenbearbeiter und der Aufsicht des EDÖB; soweit sie vom Bund als Nationale Zuteilungsstelle für Organtransplantationen im Sinne der Transplantationsgesetzgebung eingesetzt ist, untersteht sie den Vorschriften des DSG für Bundesorgane und ebenfalls der Aufsicht des EDÖB. Betreibt die Stiftung zudem eine Plattform, auf der die beteiligten kantonalen Spitäler und Transplantationszentren für ihre eigenen Aufgaben Personendaten bearbeiten (lassen), so müssen diese Datenbearbeitungen den Anforderungen des jeweiligen kantonalen Datenschutzrechts genügen und sie werden von den kantonalen Datenschutzbehörden beaufsichtigt.

4 Aufgaben der Datenschutzaufsichtsstelle

Die gesetzlichen Aufgaben der DSA sind in Artikel 34 KDSG im Einzelnen aufgelistet. Wir verstehen ihren 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 beabsichtigten elektronischen Datenbearbeitungen mit besonderen Risiken für die betroffenen Personen (Vorabkontrolle). Zudem führt sie Informationssicherheitsprüfungen von in Betrieb stehenden Systemen und Applikationen (Audits) durch. Für betroffene Personen steht die DSA als Anlaufstelle für Beratung, Vermittlung und die Behandlung von Beschwerden zur Verfügung. Erweist es sich zur Durchsetzung eines angemessenen Datenschutzes als unvermeidbar, 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 – welche als Form der präventiven Aufsicht im Vordergrund steht und im Hinblick auf vermehrt agil geführte Informatikprojekte zusätzlich an Bedeutung gewinnen dürfte – keinen Erfolg verspricht. Mit dem Register über die von kantonalen Behörden geführten Datensammlungen schafft die DSA Transparenz, damit die betroffenen Personen ihre Rechte auf Auskunft und Einsicht (sowie ggf. Berichtigung oder Löschung) wahrnehmen können.

5 Organisation / Ressourcen / Netzwerk

Per 31. Dezember 2024 verfügte die DSA über einen Personalbestand von 670 %, aufgeteilt auf acht Personen. Davon sind fünf Personen juristisch ausgebildet, drei Personen sind Informatiker bzw. Informatikprüfer:

Ueli Buri (Datenschutzbeauftragter) 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 seit über 10 Jahren für den Kanton Bern in der Rolle als interner Informatik-Revisor tätig. Seine Hauptaufgabe in der DSA umfasst die Planung und Durchführung von Prüfungen von in Betrieb stehenden IT-Systemen und Anwendungen sowie die Begleitung der Umsetzung von organisatorischen und technischen Massnahmen im Bereich der Informationssicherheit und des Datenschutzes (ISDS).

Rahel Lutz (stellvertretende Datenschutzbeauftragte Recht) ist Rechtsanwältin und arbeitet seit 2009 bei der DSA. Sie betreut die Gesundheits-, Sozial- und Integrationsdirektion (GSI) in datenschutzrechtlichen Fragen. In Vorabkontrollen prüft sie die eingereichten ISDS-Dokumente hinsichtlich rechtlicher Aspekte.

Liz Fischli-Giesser (wissenschaftliche Mitarbeiterin Recht) ist Fürsprecherin und arbeitet seit 2012 bei der DSA. Sie ist hauptsächlich zuständig für den Datenschutz bei der Finanzdirektion (FIN) sowie der Wirtschafts-, Energie- und Umweltdirektion (WEU), bei Videoüberwachungen und bei Fragen von Kirchgemeinden.

Christina Hug Gnägi (wissenschaftliche Mitarbeiterin Recht) ist Rechtsanwältin und arbeitet seit dem Frühjahr 2024 bei der DSA. Sie betreut hauptsächlich Beratungs-, Gesetzgebungs- und Vorabkontrollgeschäfte im Aufgabenbereich der GSI (Verwaltung und Gesundheitseinrichtungen).

Samuel Kaufmann (wissenschaftlicher Mitarbeiter Informatik) ist seit 2016 in der IT-Entwicklung und seit 2023 bei der DSA im Bereich der technischen Vorabkontrollen tätig.

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

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

Im Rahmen der Totalrevision des KDSG soll die Datenschutzberatung und -aufsicht für die meisten Gemeinden an die DSA übertragen werden (siehe dazu auch Ziff. 6.2 und 6.5.3). Laut den Angaben des Amtes für Gemeinden und Raumordnung bestanden im November 2024 insgesamt 335 Einwohner- und gemischte Gemeinden, 182 Burgergemeinden und 241 Kirchgemeinden. Zur Wahrnehmung der neuen Aufgabe ab dem Jahr 2026 benötigt die DSA vier zusätzliche Vollzeitstellen, für die sie – um das Personal gestaffelt anstellen und ausbilden zu können – die halben Kosten in das Budget 2025 eingestellt hatte. Weil der Gesetzesentwurf im Zeitpunkt der Vorberatung des Budgets noch nicht verabschiedet war, lehnten die Finanzkommission und auf deren Antrag der Grosse Rat die Erhöhung des Stellenbestands vorderhand ab, weil zuerst das Gesetz beraten werden solle. Dies ist grundsätzlich nachvollziehbar, es ist aber Folgendes zu beachten: Wenn das totalrevidierte KDSG – wie aktuell geplant – in der Wintersession 2025 verabschiedet werden und im Juni 2026 in Kraft treten soll, kann die DSA nicht erst im Januar 2026 mit den zusätzlichen Rekrutierungen beginnen. Sofern der Grosse Rat in der ersten Lesung im Sommer 2025 die Aufgabenverschiebung zur DSA grundsätzlich gutheisst, muss es dieser erlaubt sein, die ersten neuen Stellen auszuschreiben und bei geeigneten Bewerbungen schon im Herbst/Winter 2025 zu besetzen. Oder aber das Übergangsrecht muss vorsehen, dass die Aufgabenverschiebung erst per 2027 wirksam wird. Andernfalls wird die DSA zunächst nicht in der Lage sein, ihre gesetzlichen Aufgaben vollumfänglich zu erfüllen.

Im Jahr 2024 betrug der Betriebsaufwand der DSA insgesamt TCHF 226. Davon wurden ca. 80 % (TCHF 180) für externe Dienstleistungen zur Unterstützung von Informatikprüfungen eingesetzt.

Innerhalb der kantonalen Verwaltung bestehen weitere Anlaufstellen, welche die verantwortlichen Behörden in ISDS-Fragen beraten: So verfügen die Direktionen und die STA je über mindestens eine Kontaktstelle für Datenschutz, die ihre Ämter berät, und eine(n) Informationssicherheitsverantwortliche(n) (I-SIVE). Die Gemeindebehörden können sich mit allgemeinen Datenschutzfragen an das Amt für Gemeinden und Raumordnung sowie mit fachspezifischen Fragen (z. B. betreffend die Digitalisierung der Volksschule) an die Direktionen und die STA wenden. Mit Blick auf ihr Ziel, das Bewusstsein und Wissen im Bereich des Datenschutzes bei allen Behörden zu erweitern, führte die DSA im Berichtsjahr einerseits einen weiteren Anlass mit allen Kontaktstellen für Datenschutz durch, um das Thema der Datenbekanntgabe durch Behörden fachlich vertieft zu präsentieren und diskutieren. Anderseits bot sie auf Einladung der betreffenden I-SIVE Einführungen in den Datenschutz für Mitarbeitende der DIJ, der FIN und der STA.

Mit Behörden, bei deren Tätigkeiten sich regelmässig anspruchsvolle datenschutzrechtliche Fragen stellen (Beispiele: Amt für Informatik und Organisation [KAIO], Bedag AG, Kantonspolizei [KAPO], Insel Gruppe AG und weitere Gesundheitseinrichtungen), pflegt die DSA institutionalisierte Kontakte.

Im Hinblick auf einen gesamtstaatlich abgestimmten ISDS-Auditplan pflegen ausserdem die Finanzkontrolle des Kantons Bern und die DSA eine verstärkte strategisch ausgerichtete Zusammenarbeit.

Als Mitglied von «privatim», der Konferenz der schweizerischen Datenschutzbeauftragten, steht die DSA in regelmässigem Kontakt zu den anderen kantonalen Aufsichtsstellen und zum EDÖB. Dabei geht es einerseits um den Wissens- und Erfahrungsaustausch in Fragen, welche sich in allen Kantonen gleichermassen stellen, und andererseits um die Koordination der Aufsichtstätigkeit bei der kantonsübergreifenden Zusammenarbeit der Behörden. Der Leiter der DSA ist Mitglied im Büro (Vorstand) und seit November 2020 Präsident von privatim, die stellvertretende Datenschutzbeauftragte Recht leitet die Arbeitsgruppe Gesundheit. In den übrigen fachbezogenen Arbeitsgruppen (zurzeit Digitale Verwaltung, Sicherheit und ICT) nimmt je eine Person der DSA teil. Siehe für Einzelheiten zu den im Berichtsjahr bearbeiteten Themen die Ziff. 6.6 unten.

6 Fachliche Berichterstattung aus dem Arbeitsalltag

Die folgende Berichterstattung stellt eine Auswahl von Geschäften aus allen Aufgabenbereichen der DSA dar, welche entweder von besonderer fachlicher Bedeutung oder für die jeweilige Aufgabe besonders illustrativ sind.

6.1 Beratung

6.1.1 Behörden

Angemessenes Datenschutzniveau bei der Übermittlung von Personendaten in die USA

Nach dem Vorbild der Europäischen Union vereinbarte die Schweiz mit den USA das *Swiss-U.S. Data Privacy Framework* (CH-US Datenschutzrahmen), nach dem sich Unternehmen in den Vereinigten Staaten zertifizieren lassen können, wenn sie eine Reihe von Datenschutzverpflichtungen einhalten. Gestützt auf jenen Datenschutzrahmen stellte der Bundesrat im August 2024 fest, dass bei der Übermittlung von Personendaten an zertifizierte US-Unternehmen ein angemessener Datenschutz bestehe. Zwar orientiert sich das KDSG, das für die Übermittlung von Personendaten ins Ausland (insbesondere bei der Nutzung von ausländischen Cloud-Services) ebenfalls einen angemessenen Schutz im Zielland verlangt, nicht ausdrücklich am Bundesrecht, es bietet sich aber an, auf dieses abzustellen. Das KAIO unterbreitete seine betreffende Information an die Kantonsverwaltung vorgängig der DSA zur Stellungnahme. Diese wies darauf hin, dass, weil die US-Unternehmen ihre Zertifizierung jederzeit selbst widerrufen können, zwei Massnahmen getroffen werden müssen, damit US-Cloud-Services genutzt werden können: Erstens ist sicherzustellen, dass der Bestand der Zertifizierung regelmässig überprüft wird, damit ein Wegfall zeitnah festgestellt werden kann. Und zweitens ist für diesen Fall ein Ausstiegsszenario bereitzuhalten, damit die Nutzung des Cloud-Services umgehend eingestellt werden kann.

Erstellung eines Bloomfilters bei einer «Trusted Third Party»

Ein Institut der Universität Bern (UniBE) prüfte, ob Ärztinnen und Ärzte Patientendaten mittels einer «Trusted Third Party» anonymisieren dürfen. Dabei wäre aus den Patientenangaben «Name», «Vorname», «Geburtsdatum» und «Geschlecht» durch eine Hilfsperson ein Hashwert (d. h. ein eindeutiger numerischer Wert) generiert worden. Dieser wäre zusammen mit weiteren Angaben zur Erkrankung an das Institut übermittelt worden. Dieses hätte keine Möglichkeit gehabt, die betroffenen Personen zu re-identifizieren, aber dennoch sicherstellen können, keine doppelten Datensätze zu erhalten.

Ärztinnen und Ärzte sind datenschutz- und strafrechtlich verpflichtet, Informationen vertraulich zu behandeln und Geheimnisse zu schützen. Der Einsatz von Hilfspersonen ist erlaubt, erfordert jedoch deren sorgfältige Auswahl, Instruktion und Kontrolle. Diese Pflichten sollten vertraglich geregelt werden, um die Hilfspersonen zur Verschwiegenheit über die anvertrauten Geheimnisse zu verpflichten. Im Rahmen der von der DSA begleiteten Abklärungen zur Lösung mit einer «Trusted Third Party» stellte sich daher die Frage, wie Ärztinnen und Ärzte ihrer Verpflichtung zur sorgfältigen Auswahl, Instruktion und Kontrolle der Hilfsperson nachkommen könnten, ohne das Risiko einzugehen, Geheimnisse preiszugeben und sich dadurch möglicherweise strafbar zu machen. Letztlich entschied sich die Behörde gegen diese skizzierte Lösung.

Aufsichtsrechtliche Zuständigkeit für medizinische Register

Die DSA und der EDÖB prüften gemeinsam mit der UniBE das anwendbare Datenschutzrecht und die datenschutzrechtliche Aufsichtszuständigkeit der jeweiligen Behörde für die von der UniBE gesamtschweizerisch geführten medizinischen Register. Dabei wurden vier Bearbeitungskonstellationen unterschieden: Die UniBE kann eigene Forschung betreiben, es kann ihr eine öffentliche Aufgabe des Kantons oder des Bundes übertragen worden sein oder sie handelt im Auftrag von Privaten. Für jede Konstellation wurden das anwendbare Datenschutzrecht und die zuständige Aufsichtsbehörde festgelegt sowie die geführten Register zugeordnet. Damit konnten sowohl die rechtlichen Zuständigkeiten als auch die Registerzuordnungen für jede Bearbeitungskonstellation klar definiert werden.

Bekanntgabe von Daten der Gebäudeversicherung Bern an Steuerbehörden

Die Steuerverwaltung prüft im Hinblick auf eine Gesetzesänderung, ob der amtliche Wert von Liegenschaften künftig auf der Grundlage des Versicherungswerts bei der der Gebäudeversicherung Bern (GVB) berechnet werden soll. Zur Erarbeitung der neuen Berechnungsmethode bat sie die GVB im Rahmen der Amtshilfe um eine Auswahl von Personendaten. Auf Anfrage der WEU als Aufsichtsbehörde der GVB gelangte die DSA zur Ansicht, dass die gewünschte Datenbekanntgabe gestützt auf die bestehenden Rechtsgrundlagen – namentlich Artikel 15 KDSG, der die Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken ausdrücklich erlaubt – möglich sei. Gleichwohl beschloss die GVB aus Vorsicht, die Daten nicht an die Steuerverwaltung bekanntzugeben. Deshalb plant die FIN nun den Erlass einer «Versuchsverordnung neues amtliches Bewertungssystem», welche die GVB ausdrücklich zur Datenbekanntgabe berechtigt und verpflichtet.

Eine zweite Anfrage – diesmal von der GVB selbst – betraf die Bekanntgabe von Gebäudeversicherungswerten zur Bemessung der Zweiwohnungssteuer, welche die Gemeinden laut kantonalem Steuergesetz in einem Reglement vorsehen dürfen. Nach Ansicht der DSA stellt der Versicherungswert eines Mehrfamilienhauses mit und ohne Zweitwohnungen noch kein Personendatum dar, weil der Gesamtwert keine Aussage über eine bestimmte Person enthält. Mit dessen Offenlegung werden daher keine Daten über Personen bekanntgegeben, deren Wohnung keine Zweitwohnung darstellt und die deshalb von der Gemeinde nicht benötigt werden. Anders verhält es sich für die jeweiligen Wertquoten der Eigentümer von Zweitwohnungen. Vor deren Bekanntgabe sollte sich die GVB deshalb von der anfragenden Gemeinde zusichern lassen, dass die Werte ausschliesslich für das Berechnen der Zweitwohnungssteuer verwendet werden. Dies wurde denn in der Erläuterungen zum inzwischen verabschiedeten Reglement der betreffenden Gemeinde ausdrücklich festgehalten.

Prüfung einer materiellen Koordination mit der kantonalen Ethikkommission

Kantonale Behörden, die Forschung nach dem Humanforschungsgesetz betreiben, benötigen einerseits eine Bewilligung der kantonalen Ethikkommission und müssen andererseits, sofern die gesetzlichen Voraussetzungen erfüllt sind, ihre ISDS-Dokumentation zur Vorabkontrolle bei der DSA einreichen. Beide Behörden prüfen im Rahmen ihrer gesetzlichen Aufgaben die sichere Bearbeitung von Personendaten. Aufgrund dieser Kompetenzüberschneidung prüften die DSA und die kantonale Ethikkommission eine mögliche materielle Koordination, entschieden sich jedoch letztlich dagegen. Nur ein Bruchteil der von der kantonalen Ethikkommission bearbeiteten Gesuche hätte tatsächlich zu einer Kompetenzüberschneidung geführt, sodass eine Koordination zwischen den Behörden einen unverhältnismässig hohen Aufwand für die Ethikkommission bedeutet hätte. Im Gegenzug vereinbarten die Behörden einen intensiveren Fachaustausch.

Einwilligung der betroffenen Personen in ein niedriges Datenschutzniveau

Ein Spital ersuchte den Kantonsärztlichen Dienst um globale Befreiung von der Einhaltung der aktuell geltenden Anforderungen an die Datensicherheit, weil es mit seinen Patientinnen und Patienten via E-Mail, SMS oder WhatsApp kommunizieren wollte. Dafür sollten die betroffenen Personen eine Einwilligungserklärung unterzeichnen. Die DSA beurteilte die generelle Absenkung der Datensicherheitsstandards gestützt auf eine Einwilligung aller betroffener Personen mangels einer gesetzlichen Grundlage als nicht zulässig. Im Rahmen des Rechts auf informationelle Selbstbestimmung ist zwar eine Einwilligung der Betroffenen in engen Schranken möglich, dies darf aber nicht zur Folge haben, dass eine Behörde generell auf die gesetzlich verlangten Sicherheitsmassnahmen verzichtet, weil

diesfalls die für eine gültige Einwilligung verlangte Freiwilligkeit nicht mehr gegeben ist. Eine ungesicherte Kommunikation von Gesundheitsdaten darf nur dann erfolgen, wenn die betroffene Person aus eigener Initiative ausdrücklich darum bittet.

Bekanntgabe von Initialen an Apotheken zur Bekämpfung von Rezeptfälschungen

Eine Apotheke in Grenznähe des Kantons Bern erkundigte sich bei der DSA, warum sie zwecks Bekämpfung von Rezeptfälschungen vom pharmazeutischen Dienst des Kantons Bern nur die Initialen von Personen mitgeteilt erhalte, die ein gefälschtes Rezept einzulösen versuchten. Von den pharmazeutischen Diensten des eigenen und eines angrenzenden Kantons würden vollständige Namensangaben geliefert. Die Abklärung der DSA ergab, dass die Berner Apothekerinnen und Apotheker gesetzlich verpflichtet sind, gefälschte ärztliche Verschreibungen nicht auszuführen und dem Gesundheitsamt zu melden. Jedoch fehlt eine Rechtsgrundlage dafür, dass der pharmazeutische Dienst die erhaltenen Informationen an sämtliche bernischen und grenznahen Apotheken zwecks Alarmierung weiterleiten darf. Die Bekanntgabe der Initialen erscheint der DSA als pragmatischen und zulässigen Weg, um trotzdem einen Alarm abzugeben. Bei der Bekanntgabe der Initialen handelt es sich um ein Pseudonym, bei dem der «Schlüssel» für die Zuordnung zu einer bestimmten Person beim pharmazeutischen Dienst verbleibt. Nur wenn die betroffene Person das gefälschte Rezept einlösen will, wird das Pseudonym durch sie selbst aufgelöst. Andenfalls – und damit in den meisten Fällen – verbleibt die Alarmmeldung ohne Personenbezug.

Microsoft Bing Copilot im Unterricht des Inforama

Das Amt für Landwirtschaft und Kultur wandte sich mit der Frage an die DSA, ob der Microsoft Bing Copilot (ehemals Bing Chat Enterprise BCE) im Lernbetrieb des Inforama von Lehrpersonen und Lernenden eingesetzt werden darf. Der Bing Copilot gehört zu den generativen Anwendungen der Künstlichen Intelligenz (KI), mit dessen Hilfe Textinhalte erzeugt werden können. Die Abklärungen ergaben, dass die Benutzer- und Unternehmensdaten bei der lizenzierten Enterprise-Version geschützt sind und keine Chatdaten gespeichert werden. Die DSA kam zum Schluss, dass der dokumentierte Bing Copilot im Rahmen der bestehenden Lizenzen für Microsoft 365 (M365) genutzt werden kann, sofern mittels Nutzungsbestimmungen sichergestellt wird, dass bei seinem Gebrauch keine Personendaten eingegeben werden. In der Folge nahm das Inforama entsprechende Vorschriften in die «Nutzungsanweisung für den Umgang mit interaktiven Applikationen» für Mitarbeitende, Lehrpersonen und Lernende auf.

Ausdrückliche Rechtsgrundlage für Abrufverfahren aus eBau?

Das Amt für Umwelt und Energie (AUE) benötigt beim Vollzug des kantonalen Energiegesetzes und für Aufgaben im Bereich der Luftreinhaltung Sach- und Personendaten, die von den Gemeinden im System für das elektronische Baubewilligungsverfahren (eBau) erfasst wurden. Das AUE fragte die DSA an, welche Art von Rechtsgrundlage für den Abruf der Daten aus eBau erforderlich sei. Für die Bekanntgabe von Personendaten im Einzelfall (Amtshilfe) genügt es grundsätzlich, wenn die empfangende Behörde eine gesetzliche Aufgabe wahrnimmt, zu deren Erfüllung sie die angefragten Personendaten benötigt. Mit der Kontrolle der Feuerungsanlagen und der Erfassung von Meldungen über einen Heizungsersatz erfüllt das AUE gleich zwei Aufgaben, für die es die Personendaten benötigt. Falls der Zugang zu den Daten im Abrufverfahren verhältnismässig ist und für die betroffenen Personen keine besonderen Risiken bestehen, muss das Abrufverfahren nicht notwendigerweise ausdrücklich geregelt sein. Die DSA wies aber darauf hin, dass die (bei besonders schützenswerten Daten zwingende) Erforderlichkeit der Daten für die Aufgabenerfüllung qualifiziert dargelegt werden muss, damit ein Abrufverfahren als zulässig erscheint. Aus Gründen der Rechtssicherheit und der Transparenz über die Datenbearbeitung unterstützt die DSA generell die Schaffung einer ausdrücklichen Regelung, wobei für normale Personendaten eine Regelung in einer Verordnung genügt.

6.1.2. Betroffene Personen

Adressbekanntgabe an Miterben trotz Adresssperre

Eine Bewohnerin der Stadt Bern hatte bei der Einwohnerkontrolle die Bekanntgabe ihrer Daten an private Personen sperren lassen. Im Zusammenhang mit dem Tod ihres Vaters erliess das Regierungsstatthalteramt (RSTA) Bern-Mittelland eine Verfügung und schickte diese in Kopie allen Erben unter Angabe aller vollständigen Postadressen. Dies wurde von der betroffenen Person mit einer aufsichtsrechtlichen Anzeige bei der DSA gerügt. Deren Abklärungen ergaben Folgendes: Das RSTA hat nach dem Tod eines Erblassers einen ersten Kontakt mit den erbberechtigten Personen aufzunehmen und der Erbengemeinschaft erste Rechte und Pflichten (z. B. eine Urkundsperson vorzuschlagen) zu übertragen. Als sog. Gesamthandschaft kann eine Erbengemeinschaft nur mit der Mitwirkung aller Erben handeln, weshalb diese Kenntnis von den anderen Erben haben und diese erreichen können müssen. Vor diesem Hintergrund war die Adressbekanntgabe trotz Datensperre rechtmässig. In besonderen Situationen können überwiegende Interessen der betroffenen Person (z. B. deren Gefährdung) die Datenbekanntgabe ausschliessen. Falls zusätzlich zur Adresssperre entsprechende Anhaltpunkte bestehen, muss das RSTA vor der Datenbekanntgabe die Person anhören, damit es eine umfassende Interessenabwägung vornehmen kann.

Prüfung der Notwendigkeit der Angaben in Gesundheitsfragebogen

Eine Privatperson liess in den zahnmedizinischen Kliniken der UniBE (ZMK) eine Dentalhygiene-Behandlung durchführen und beanstandete anschliessend bei der DSA den umfassenden Gesundheitsfragebogen, den sie ausfüllen musste. Die DSA prüfte den Sachverhalt, holte eine Stellungnahme der ZMK ein und kam zu folgendem Schluss: Eine Dentalhygiene ist in den meisten Fällen mit einem zahnärztlichen Befund verbunden und stellt somit eine zahnärztliche Behandlung dar. Obwohl die Dentalhygiene grösstenteils von speziell geschultem Personal in Delegation durchgeführt wird und nicht direkt von der Zahnärztin oder dem Zahnarzt selbst, bleiben die Aufnahme- und Anamnesebögen unverändert. Die Bearbeitung der im Gesundheitsfragebogen enthaltenen Informationen im Rahmen der Dentalhygiene ist für die ZMK daher zwingend erforderlich und datenschutzrechtlich nicht zu beanstanden.

Veröffentlichung von Gemeindeversammlungsprotokollen

Obwohl die Gemeinden des Kantons Bern noch über eigene Datenschutzaufsichtsstellen verfügen (siehe Ziff. 6.5.3), gab die DSA bei Anfragen von Bürgerinnen und Bürgern allgemeine Auskünfte. Dazu gehörte die Feststellung, dass es erlaubt sei, Gemeindeversammlungsprotokolle auf der Webseite der Gemeinde aufzuschalten. Nach dem Gesetz über die Information und die Medienförderung (IMG) sind Gemeindeversammlungen öffentlich, und das Gemeindegesetz verpflichtet die Gemeinden, über die Versammlungen ein Protokoll zu führen. Wiederum nach dem IMG informieren die Behörden von Amtes wegen über Tätigkeiten von allgemeinem Interesse und nutzen dafür vorzugsweise das Internet. Die Information ist insoweit einzuschränken, als überwiegende öffentlichen oder private Interessen entgegenstehen, namentlich weil besonders schützenswerte Personendaten betroffen sind.

Geburtstagsjubiläum: Bekanntgabe des Jahrgangs in Dorfzeitschrift

In der Dorfzeitschrift einer Gemeinde wurde allen Einwohnerinnen und Einwohnern ab 75 Jahren zum Geburtstag gratuliert und dabei das Geburtsdatum publiziert. Die aufsichtsrechtliche Anzeige einer betroffenen Person leitete die DSA zuständigkeitshalber an die kommunale Aufsichtsstelle weiter und brachte zu deren fachlichen Unterstützung folgende Hinweise an: Das KDSG erlaubt es den Gemeinden, in ihren Reglementen die systematisch geordnete Bekanntgabe bestimmter Daten (sog. Listenauskünfte) vorzusehen. Das Datenschutzreglement der betreffenden Gemeinde sieht Listenauskünfte an die Redaktion der Zeitschrift zum Zweck von Geburtstagsgratulationen ausdrücklich vor. Jedoch dürfen nur die im KDSG genannten Angaben weitergegeben werden, vorliegend der Jahrgang und nicht das vollständige Geburtsdatum. Die kommunale Aufsichtsstelle sollte deshalb die Einwohnerkontrolle anweisen, künftig nur noch die erlaubten Angaben

bekanntzugeben. Zudem sollte die verantwortliche Einwohnerkontrolle von der Redaktion verlangen, dass diese die Geburtsdaten vollständig aus ihren Datenbeständen löscht und die bisherigen Publikationen aus dem Internet entfernt.

Verschlüsselte E-Mail-Kommunikation bei besonderen Geheimhaltungspflichten

Eine Privatperson störte sich daran, dass ein Notar ihr Vertragsentwürfe mit unverschlüsselter E-Mail übermittelte, und erkundigte sich bei der DSA nach der Zulässigkeit. Im Rahmen ihrer hauptberuflichen Tätigkeit gelten Berner Notarinnen und Notare als Behörden und unterstehen dem KDSG. Dieses macht die zu treffenden Schutzmassnahmen vom Risiko für die betroffene Person abhängig. Besonders schützenswerte Personendaten dürfen grundsätzlich nur verschlüsselt übermittelt werden. Aus Datenschutzsicht kommt es somit auf den konkreten Vertragsinhalt an, ob die E-Mail verschlüsselt werden muss oder nicht. Allerdings unterstehen Notarinnen und Notare auch dem Berufsgeheimnis nach dem Schweizerischen Strafgesetzbuch. Dieses verlangt nach Lehre und Rechtsprechung generell – also unabhängig vom konkreten Inhalt – eine verschlüsselte Kommunikation. Hätte die Privatperson aus eigener Initiative im Einzelfall eine unverschlüsselte Kommunikation gewünscht, wäre diese zulässig gewesen (siehe Ziff. 6.1.1). Andernfalls sind von einer besonderen Geheimhaltungspflicht erfasste Angaben unabhängig von ihrer datenschutzrechtlichen Qualifikation verschlüsselt zu übermitteln.

Sichtbarkeit des Status in MS Teams der Kantonsverwaltung

Ein Kantonsmitarbeiter erkundigte sich bei der DSA, ob es zulässig sei, dass in der neuen Applikation MS Teams sein jeweils aktueller Status («verfügbar», «beschäftigt», «abwesend» und dergl.) für die Vorgesetzten – übrigens auch für das übrige Kantonspersonal – einsehbar und damit eine totale Überwachung möglich sei. Mit Blick auf die Einsehbarkeit der Kalendereinträge in MS Outlook hatte die DSA verlangt, dass jene standardmässig deaktiviert ist und jede Person aktiv einstellen muss, für wen was (nichts, nur Frei-/Gebucht-Zeiten, Betreff/Ort, Inhalte) sichtbar ist. Der Kalender unterscheidet sich in zwei wichtigen Punkten von Teams: Erstens handelt es sich primär um ein Instrument zur eigenen Arbeitsorganisation und nicht um ein Kommunikationsmittel, und zweitens können Kalendereinträge über den gesamten Zeitverlauf – d.h. für die Vergangenheit und die Zukunft – konsultiert werden, so dass gegebenenfalls sehr viel mehr Informationen offengelegt werden als mit dem momentanen Teams-Status. Demgegenüber ist Teams ein Kommunikationsmittel, wobei die aktuelle Erreichbarkeit der Kantonsmitarbeitenden eine sachdienliche Information darstellt. Weil immer nur der jeweilige Status angezeigt wird, müssten Dritte eine bestimmte Person ständig beobachten, um ein «Arbeitsprofil» erstellen zu können. Vor allem aber kann jede Person ihren Status jederzeit manuell übersteuern und damit bestimmen, welcher

Status von Teams angezeigt wird.

Keine Pflicht zur Meldung einer E-Mail-Adresse an die Einwohnergemeinde

Gestützt auf die Verordnung über Niederlassung und Aufenthalt der Schweizerinnen und Schweizer (NAV) können die Gemeinden seit Februar 2024 die E-Mail-Adresse der Einwohnerinnen und Einwohner erheben und verwenden. Deshalb bat eine Gemeinde jene in ihrem Mitteilungsblatt darum, die E-Mail-Adresse zu melden, damit die tägliche Post und die Gebührenrechnungen der Gemeinde nur noch elektronisch zugestellt werden können. Dies veranlasste einen Bürger zur Anfrage an die DSA, ob es zulässig sei, dass die Gemeinde nur noch elektronisch kommunizieren wolle, und ob er verpflichtet sei, seine E-Mail-Adresse zu melden. Letzteres ist nicht der Fall: Die NAV schafft für die Gemeinden eine neue Möglichkeit, jedoch keine neuen Pflichten für die Einwohnerinnen und Einwohner. Im Vortrag zur Änderung der NAV steht klar: «Selbstverständlich ist damit für die anmeldende Person keine Pflicht verbunden, zwingend eine E-Mail-Adresse zu führen oder ein Mobiltelefon zu besitzen oder diese tatsächlich bekannt zu geben. Die Führung dieser Daten ermöglicht den Gemeinden bei Bedarf jedoch eine rasche und unkomplizierte Kontaktaufnahme mit den Betroffenen».

6.1.3. Weiterbildung

Mitwirkung der DSA bei der Ausbildung von Gemeindepersonal

Das Bildungszentrum für Wirtschaft und Dienstleistung bwd bietet verschiedene Lehrgänge und Kurse für Mitarbeitende von Gemeindebehörden an. Seit vielen Jahren – auch im Berichtsjahr – unterrichten Mitarbeitende der DSA das Fach «Datenschutz und Informationssicherheit» im Rahmen der Lehrgänge zur Erlangung des Fachausweises als Bernische/r Gemeindefachfrau/mann, für Mitarbeitende der Schuladministration und für Mitarbeitende von Kirchgemeindesekretariaten an. Seit 2021 bietet die DSA zudem eine spezifische Ausbildung für Kirchgemeindebehörden zum Thema «Datenschutz in Kirchgemeinden» an. An den Kursen erläutern die Vertreterinnen und Vertreter der DSA einerseits die allgemeinen Grundsätze des Datenschutzrechts und deren Anwendung im Fachbereich der Kursteilnehmenden, andererseits ist auch die Diskussion und Beantwortung konkreter Fragestellungen aus deren Arbeitsalltag ein wichtiges Anliegen.

Im Frühjahr 2024 wirkte der Datenschutzbeauftragte erstmals an der neuen Weiterbildung für das französische Gemeindepersonal des Centre de formation

professionelle Berne francophone (ceff) in Tramelan mit, bei welcher der Datenschutz und die Informationssicherheit als Prüfungsfach gelten.

Weitere Vorträge der DSA für Mitarbeitende der Gemeinden erfolgten an einem Seminar der KPG Bern, der Medien und Informatik-Konferenz der Abteilung Schulen der Stadt Biel sowie einem Netzwerkanlass des RSTA Bern-Mittelland.

Wissensvermittlung im Rahmen von spezifischen Anlässen

Vertreter der DSA nahmen auf Anfrage an verschiedenen Weiterbildungsanlässen und Fachkonferenzen teil und referierten teils über die Grundsätze des Datenschutzrechts (Weiterbildungsanlass Mittelschul- und Berufsbildungsamt, Konferenz der Berufsfachschulen Bern, Gymnasium Neufeld) und teils über spezifische Themen (Datenschutz im Beschaffungskontext an einem Fachaustausch von Educa, Datenbekanntgabe im In- und ins Ausland am 17. Schweizerischen Datenschutzrechtstag der Universität Freiburg sowie Datenaustausch mit interkantonalen [privaten] Leistungserbringern am Schulthess Forum Datenschutz in Städten und Gemeinden 2024).

Handbuch Informationsaustausch unter Behörden

Das Handbuch Informationsaustausch unter Behörden von 2012 wurde überarbeitet und im November 2024 auf der Webseite der DSA publiziert. Es soll den Behörden auf kantonaler und kommunaler Ebene als möglichst verständliche Anleitung dienen, wann und wie sie Informationen untereinander austauschen dürfen, sollen oder müssen.

6.2 Formelle Stellungnahmen

Totalrevision des Kantonalen Datenschutzgesetzes

Nach der Vernehmlassung zum Vorentwurf für eine Totalrevision des KDSG im Vorjahr erhielt die DSA im Berichtsjahr die Gelegenheit, sich im zweiten Mitberichtsverfahren erneut zum Geschäft zu äussern. Trotz sehr zahlreicher – grösstenteils rechtstechnischer – Anträge zu Gesetz und Vortrag konnte die DSA feststellen, dass sie die Vorlage insgesamt als sehr sorgfältig erarbeitet und in den wesentlichen Punkten als ausgereift erachtete. Zum vom Regierungsrat am 13.11.2024 zuhanden des Grossen Rats verabschiedeten Gesetzesentwurf hat die DSA im Wesentlichen die nachfolgenden Bemerkungen.

Das von der DSA geführte Register der Datensammlungen der kantonalen Behörden soll künftig nur noch Datenbestände mit besonders schützenswerten Personendaten enthalten. Damit erhofft sich die Verwaltung eine Reduktion ihres administrativen Aufwands. Das online einsehbare Register ist für die betroffenen Personen ein wichtiger Ausgangspunkt für die Wahrnehmung des verfassungsmässigen Rechts auf Einsicht in ihre Daten und gegebenenfalls deren Berichtigung oder Löschung, sofern sie nicht (mehr) benötigt werden. Dieses Recht besteht für alle Personendaten unabhängig von deren Schutzwürdigkeit. Bei einer Beschränkung des Registers auf sensitive Daten entfällt die Möglichkeit der Bürgerinnen und Bürger, sich selbständig über die bestehenden Datensammlungen, deren Rechtsgrundlage, den Bearbeitungszweck und die Weitergabe der Daten an Dritte zu erkundigen. Ausserdem ist zu beachten, dass die Behörden künftig umfassender über die von ihnen beschafften Personendaten informieren müssen. Sie kann auf die Information verzichten, wenn die betroffenen Personen bereits über die nötigen Angaben verfügen, etwa weil diese aus dem Register der Datensammlungen ersichtlich sind. Werden Datensammlungen ohne besonders schützenswerte Personendaten künftig nicht mehr im Register geführt, verschiebt sich der Aufwand der Behörden von der Meldung der Datensammlung zur Information der betroffenen Personen im Einzelfall.

Im Register sollen neu auch von den Behörden eingesetzte algorithmische Entscheidsysteme mit hohem Risiko für die betroffenen Personen ausgewiesen werden. Auf die Regelung einer Informationspflicht im Rahmen von automatisierten Einzelfallentscheidungen, die sich auf die betroffene Person erheblich auswirken kann, wurde jedoch verzichtet. Der Regierungsrat geht davon aus, dass solche Entscheidungen immer formelle Verfügungen darstellen, weshalb die Informationspflicht im Verwaltungsrechtspflegegesetz zu verankern sei. Demgegenüber regelte der Bund die von der revidierten Europaratskonvention vorgeschriebene Informationspflicht im neuen DSG. Zwar schrieb auch der Bundesrat in seiner Botschaft, dass solche Entscheidungen «grundsätzlich» als Verfügungen ergehen, in der Literatur zum DSG ist man sich aber einig, dass die Informationspflicht auch für andere automatisierte Einzelfallentscheidungen gilt. Sie soll es der betroffenen Person ermöglichen, die Entscheidung von einem Menschen überprüfen zu lassen. Tatsächlich gibt es zahlreiche Bereiche, in denen die Behörden Entscheidungen treffen, die keine Verfügungen darstellen und die künftig unter Einsatz von KI getroffen werden können (zumal teils bereits entsprechende Anwendungen bestehen). Dazu gehört die Triage von Stellenbewerbungen auf geeignete und ungeeignete Kandidatinnen und Kandidaten, die automatisierte Korrektur und Benotung von Tests (z. B. in der Schule) sowie die Beurteilung der Gefahr einer Straftat durch eine konkrete Person («predictive policing») oder der Rückfälligkeit eines Straftäters. Die DSA hält deshalb eine Informationspflicht nur im Rahmen von formellen Verfügungen nicht für ausreichend.

Totalrevision des Sozialhilfegesetzes

In der Vernehmlassung zur Totalrevision des Sozialhilfegesetzes nahm die DSA ausführlich Stellung und publizierte ihre Eingabe später nach mehrmaliger Nachfrage und in Absprache mit der federführenden GSI auf ihrer Webseite. Neben rechtstechnischen und gesetzessystematischen Hinweisen zur besseren Verständlichkeit der Vorlage wies die DSA namentlich darauf hin, dass die Mitarbeitenden der Sozialdienste zwar dem Sozialhilfegeheimnis, nicht aber dem ärztlichen Berufsgeheimnis unterstehen, wenn sie Informationen von Gesundheitsfachpersonen erhalten. Gleichwohl ist vor einer allfälligen Weitergabe der Informationen an Dritte eine Interessenabwägung vorzunehmen und der Geheimhaltungspflicht der Gesundheitsfachperson besonderes Gewicht beizumessen. Weiter wurde darauf hingewiesen, dass bei einer Auswertung von Personendaten anhand der AHV-Nummer anstelle des Namens nicht mehr von einer «Pseudonymisierung» gesprochen werden könne (siehe sogleich unten); stattdessen sei hier – wie bei der Auswertung von Randdaten nach der Personalgesetzgebung – von einer personenbezogenen, aber nicht namentlichen Datenbearbeitung zu sprechen. Dass die GSI zur Beantwortung parlamentarischer Vorstösse oder zu Kommunikationszwecken auf einzelne Sozialhilfedossiers zugreifen können soll, erachtete die DSA als unzulässig.

Änderung der Transplantationsverordnung

Im Rahmen der Vernehmlassung des Bundes zur Änderung der Transplantationsverordnung wurde die DSA zur Stellungnahme des Kantons Bern konsultiert. Auf ihren Antrag hin hielt der Regierungsrat in seiner Eingabe fest, dass die Einsicht der Mitarbeitenden des Bundesamtes für Gesundheit in Daten mit der AHV-Nummer als Personenidentifikator nicht als Zugang nur zu pseudonymisierten Daten bezeichnet werden könne. Inzwischen wird die AHV-Nummer in so vielen Verwaltungsbereichen – unter anderem im Grundbuch und im Strafregister – systematisch als Personenidentifikator verwendet, dass sie den Anforderungen an eine wirksame Pseudonymisierung nicht mehr standhält, weil die Zuordnung zu einer bestimmten Person für zu viele Akteure möglich ist.

Zugang zur Zentralen Personenverwaltung für Notarinnen und Notare

Zur Erfüllung ihrer behördlichen Aufgaben können bernische Notarinnen und Notare seit mehreren Jahren bestimme Daten von der Gemeinderegistersysteme-Plattform (GERES) abrufen. Diese enthält aber nur natürliche Personen mit Wohnsitz im Kanton Bern und weder juristische Personen noch ausserkantonale Grundeigentümerinnen. Deshalb sollte die Möglichkeit geschaffen werden, dass die Notarinnen und Notare auch Zugang zur Zentralen Personenverwaltung (ZPV) der Steuerverwaltung erhalten. Während dieser Zugang fachlich unbestritten war, wachte die DSA vor allem methodisch darüber, dass die gesetzlichen Vorgaben

eingehalten wurden. Während nämlich die GERES-Verordnung den Erlass von Berechtigungsregeln vollumfänglich an die Direktionen, die STA und die Justiz delegierte, legt die ZPV-Verordnung in einem Anhang bereits grundsätzlich fest, welche Behörden welche Zugangsprofile erhalten können. Diesen Rahmen müssen die Direktionen in ihren Berechtigungsregeln einhalten. Bevor also die DIJ den Notarinnen und Notare einen Zugang zur ZPV gewähren kann, musste der Regierungsrat die ZPV entsprechend ergänzen. Die DSA geht davon aus, dass mit dem Zugang zur ZPV jener zu GERES nicht mehr erforderlich ist, so dass die DIJ die betreffende Berechtigung aufheben können wird.

Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme (POLAP-Konkordat)

Eine Motion aus dem Jahr 2018 (18.3592) verlangte vom Bundesrat, eine nationale Polizeidatenbank oder eine Vernetzungsplattform für die bestehenden kantonalen Polizeidatenbanken zu schaffen. Weil dem Bund heute die dafür nötige Gesetzgebungskompetenz fehlt, wird im Auftrag der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) an den Rechtsgrundlagen für eine nationale Abfrageplattform für Polizeidaten (POLAP) gearbeitet. Im Jahresbericht 2022 hatte die DSA im Zusammenhang mit der Revision des bernischen Polizeigesetzes (PolG) erläutert, warum sie es als hochproblematisch erachtete, in der kantonalen Gesetzgebung einseitige Ermächtigungen vorzusehen, anderen Kantonen Polizeidaten im Abrufverfahren zugänglich zu machen (S. 24). Seither hielt auch das Bundesgericht mit Blick auf das luzernische Polizeigesetz fest, dass es für das Gericht nicht ohne Weiteres ersichtlich sei, «wie ein polizeilicher Informationssystem-Verbund des Bundes und der Kantone auf der Grundlage einer Vielzahl von – u.U. divergierenden – kantonalrechtlichen Regelungen zielführend und praktikabel umgesetzt werden kann» (Urteil 1C_63/2023 vom 17.10.2024, E. 6.5). Ein besserer Weg ist ein Konkordat, an dem ebenfalls gearbeitet wird und dessen Entstehung privatim seit mehreren Jahren begleitet (siehe dazu den Jahresbericht 2023 der DSA, S. 41). Im Berichtsjahr sandte die KKJDP den Entwurf für ein solches Konkordat in die Vernehmlassung, in der auch der Kanton Bern Stellung nahm. Nach Konsultation der DSA im Mitberichtsverfahren beantragte der Regierungsrat, dass der Vereinbarungsentwurf gutachterlich auf seine Verfassungsmässigkeit hin zu untersuchen sei. «Insbesondere sind dabei die Vereinbarkeit der Vereinbarung mit der verfassungsrechtlichen Kompetenzordnung und die hinreichende Bestimmtheit der (gesetzesvertretenden) Rechtsgrundlagen für schwere Grundrechtseingriffe von Interesse». Ohne ein solches Gutachten erblicke der Regierungsrat Risiken im Ratifizierungsprozess in den 26 Kantonsparlamenten. Aus Sicht der DSA besteht zudem das Risiko, dass ein den verfassungsrechtlichen Erfordernissen nicht genügendes Konkordat vom Bundesgericht für ungültig erklärt wird.

Der Nachteil einer interkantonalen Vereinbarung wird darin gesehen, dass sie wenig flexibel ist. Einmal beschlossen und von den Mitgliedskantonen ratifiziert, ist eine Anpassung an veränderte Umstände und Bedürfnisse nur sehr schwierig zu erreichen. Der dritte – sauberste, aber auch aufwändigste – Weg besteht deshalb darin, in der Bundesverfassung eine Kompetenz des Bundes zu schaffen, um die Abfrage polizeilicher Daten unter den Kantonen sowie zwischen dem Bund und den Kantonen regeln zu können. Eine entsprechende Motion (23.4311) wurde im Juni 2024 von den eidgenössischen Räten an den Bundesrat überwiesen.

6.3 Vorabkontrollen

6.3.1. Informatikprojekte

Der DSA zur Vorabkontrolle zu unterbreiten sind geplante elektronische Datenbearbeitungen, die eine grössere Anzahl Personen betreffen (quantitatives Element) und mindestens eine der folgenden qualitativen Voraussetzungen erfüllen: Es ist zweifelhaft, ob eine genügende Rechtsgrundlage besteht, es werden besonders schützenswerte Personendaten oder Daten bearbeitet, die einer besonderen Geheimhaltungspflicht unterstehen, oder es werden technische Mittel mit besonderen Risiken für die Persönlichkeitsrechte der betroffenen Personen eingesetzt.

Im Berichtsjahr wurden insgesamt 160 Vorabkontrollen und Vorprüfungen (Vorjahr: 133) zu Informatikprojekten bearbeitet und dabei 90 (63) Geschäfte abgeschlossen.

Vorabkontrollen werden nach einem standardisierten Ablauf wie folgt durchgeführt: (1.) Eingang ISDS-Unterlagen; (2.) Vorprüfung («Eintreten»); (3.) bei Bedarf Nachbesserung durch Behörde; (4.) Anhandnahme Vorabkontrolle (rechtliche und technische Prüfung, Erstellen Berichtsentwurf mit Befunden nach Wesentlichkeit hoch, mittel oder tief); (5.) Stellungnahme Behörde zu Befunden mit hoher und mittlerer Wesentlichkeit; (6.) Prüfung, Erstellen Vorabkontrollbericht in standardisierter Form sowie Abschluss.

Klinikinformationssystem EPIC der Insel Gruppe AG

Im Berichtsjahr wurde die Vorabkontrolle des neue Klinikinformationssystems EPIC der Insel Gruppe AG mit der dritten Iteration abgeschlossen. EPIC ist ein System für die Behandlungsdokumentation, die nicht mehr am einzelnen medizinischen Fall orientiert, sondern patientenzentriert erfolgen soll. Mit dem neuen Ansatz soll die interdisziplinäre und interprofessionelle Behandlung erleichtert werden: Damit

bei Bedarf alle Standorte, Kliniken, Medizinbereiche und Berufsgruppen zusammenarbeiten können, sollen die Behandlungsdokumentationen der Patientinnen und Patienten ganzheitlich in einer Akte zentral geführt werden; auf die Daten sollen weitgehende Zugriffsrechte des medizinischen Personals bestehen. Die beim Abschluss der Vorabkontrolle offenen 10 Empfehlungen wurden per Ende des Berichtsjahres weitgehend umgesetzt. So wurde die Einwilligung der Patientinnen und Patienten, dass ihre Daten im Bedarfsfall mit anderen schweizerischen und ausländischen Spitälern, die ebenfalls EPIC benutzen, geteilt werden dürfen, massgeblich überarbeitet. Auch die Empfehlung, die vorgesehenen Kontrollmassnahmen als Kompensation zu den umfassenden Zugriffsrechten auf aktuelle und abgeschlossene Behandlungsdossiers in Betrieb zu nehmen und deren Wirksamkeit zu überprüfen, wurde grundsätzlich umgesetzt; das von der Insel Gruppe AG durchgeführte Audit zur Einhaltung der Kontrollmassnahmen ergab vier Bereiche, in denen die Kontrollen weiter verbessert werden müssen.

In EPIC integriert ist eine «Medical Content Plattform», in der den Fachpersonen medizinische Inhalte in Form von Dokumenten, Bildern, Biosignalen sowie Video- und Audiodateien zur Verfügung gestellt werden. Die Vorabkontrolle dieser Fachapplikation wurde ebenfalls mit Pendenzen abgeschlossen, deren Erledigung per Ende Berichtsjahr in Prüfung bei der DSA war.

Wie bei jeder Vorabkontrolle erfolgte auch die Prüfung von EPIC ausschliesslich dokumentenbasiert auf der Grundlage einer Selbstdeklaration der verantwortlichen Behörde (SOLL). Eine Prüfung der tatsächlichen Umsetzung (IST) der beschriebenen Massnahmen zum Schutz der Patientendaten ist nie Gegenstand der Vorabkontrolle, sondern eines allfälligen späteren Audits.

Schnittstelle für eine Datenübermittlung in das elektronische Patientendossier

Um den Einwohnerinnen und Einwohnern des Kantons Bern die Möglichkeit zu bieten, ihre in der Fachapplikation VacMe gespeicherten COVID-Impfdokumentationen automatisiert in ihr elektronisches Patientendossier übertragen zu können, wurde VacMe um eine entsprechende Schnittstelle erweitert, die als wesentliche Änderung der Fachapplikation erneut zur Vorabkontrolle zu unterbreiten war. Dabei verlangte die DSA eine unmissverständliche Klärung, dass ausschliesslich Daten zu COVID-Impfungen übertragen wurden, für die der Kanton Bern während der Pandemie die nationale Kampagne koordinierte und insoweit (bzw. ergänzt mit der Einwilligung der Patientinnen und Patienten) über eine hinreichende Rechtsgrundlage verfügte, was für andere Impfungen, für die VacMe inzwischen erweitert worden war, nicht der Fall war. Ausserdem ergaben sich zahlreiche Empfehlungen zur technischen Umsetzung, die von der federführenden GSI umgesetzt wurden.

Neues Fallführungssystem in der Sozialhilfe (Start Vorabkontrolle)

Das Programm NFFS (Neues Fallführungssystem) hat zum Ziel, ein einheitliches Fallführungssystem für die kommunalen Sozialdienste, die kantonalen Kindes- und Erwachsenenschutzbehörden sowie die Fachstellen für Integration einzuführen. Das Grossprojekt ist ein komplexes, gewichtiges, kostenintensives und zeitlich ambitioniertes Projekt der digitalen Transformation im Kanton Bern. Im neuen System sollen künftig über 85 kantonale und kommunale Behörden über eine sehr grosse Anzahl von Personen Daten bearbeiten, die als besonders schützenswert gelten, was klare gesetzliche Grundlagen voraussetzt und erhöhte Anforderungen an die technischen und organisatorischen Massnahmen zum Schutz der Daten stellt. Deshalb hatte die GSI die DSA frühzeitig beratend miteinbezogen. In einem ersten Ausbauschritt soll das System der Fallführung bei ausgewählten Sozialdiensten ausgerollt werden (sog. Pilotphase), die Einführung bei den übrigen Nutzerorganisationen soll laut aktueller Planung bis 2028 umgesetzt werden. Nach vorangegangenen intensiven Besprechungen zwischen den NFFS-involvierten Stellen der GSI und der DSA, aufgrund derer die eingereichten Unterlagen überarbeitet und präzisiert wurden, konnte die Vorabkontrolle gegen Ende des Berichtsjahres gestartet werden.

Einführung von M365 bei verschiedenen Behörden

Wie im letzten Jahresbericht (S. 27 f.) ausgeführt, bringt die Auslagerung von Datenbearbeitungen in Cloud-Dienste wegen des damit verbundenen Kontrollverlusts der verantwortlichen Behörde eine Reihe von besonderen Risiken für die Grundrechte der betroffenen Personen. Während die vertragsrechtlichen Fragen bei der Nutzung von M365 aufgrund des international gültigen Data Protection Addendum von Microsoft und der ebenfalls standardisierten Rahmenverträge und anderen Zusatzvereinbarungen behördenübergreifend beantwortet werden können, hängen zahlreiche weitere Aspekte von der konkreten Nutzung durch die jeweilige verantwortliche Behörde ab. Einerseits hat nämlich jede Behörde einen anderen gesetzlichen Auftrag, bearbeitet dabei unterschiedliche Daten (insbesondere auch von unterschiedlicher Sensitivität) und hat aufgrund der verschiedenen Fachprozesse auch unterschiedliche betriebliche Bedürfnisse. Und andererseits bedeutet eine Einführung von M365 nicht, dass künftig alle Datenbearbeitungen in der Cloud erfolgen müssen. M365 ist ein Bündel von sehr viel verschiedenen Anwendungen, welche teils weiterhin lokal genutzt (wie die bekannten Office-Programme Word, Excel und PowerPoint sowie Outlook) oder durch lokale Services (insbesondere für die Datenspeicherung) ergänzt oder ersetzt werden können.

Dass die nach dem CH-US Datenschutzrahmen zertifizierten US-Unternehmen seit Mitte September 2024 einen angemessenen Datenschutz gewährleisten, bedeutet nur, dass es nun zulässig ist, Personendaten an diese Unternehmen zu übermitteln. An den übrigen Rahmenbedingungen der Nutzung von Cloud-Diensten änderte sich nichts. Die datenschutzverantwortlichen Behörden müssen bei

der Nutzung von US-Cloud-Services gleich wie bei allen anderen Auftragsdatenbearbeitungen prüfen, ob die gesetzlichen Voraussetzungen für eine Auslagerung erfüllt werden, und sie müssen die damit verbundenen Risiken beurteilen, durch geeignete Massnahmen auf ein tragbares Mass reduzieren und die Restrisiken ausdrücklich akzeptieren.

Im Berichtsjahr unterbreiteten die KAPO und die Ausgleichskasse des Kantons Bern (AKB) der DSA ihre Vorhaben zur Einführung von M365 als Büroautomatisationslösung zur Vorabkontrolle. Wie die Kantonsverwaltung verbieten auch die KAPO und die AKB ihren Mitarbeitenden die Nutzung der Cloud-Dienste für die Bearbeitung von besonders schützenswerten Personendaten. Im Fall der AKB verbot bereits eine Weisung des Bundesamtes für Sozialversicherungen, dass Personendaten von Versicherten im Ausland bearbeitet werden, ausser es handle sich um eine Bearbeitung, die von Gesetzes wegen mit einem internationalen Datenaustausch verbunden sei. Nach Umsetzung der Empfehlungen der DSA konnten beide Vorhaben grundsätzlich als datenschutzkonform beurteilt werden.

Die Bernische BVG- und Stiftungsaufsicht (BBSA) plante ebenfalls eine Migration zu M365 und reichte die betreffenden Unterlagen zur Vorabkontrolle ein. Es stellte sich die Frage, ob die E-Mail-Lösung «Exchange Online» als Cloud-Service bezogen werden dürfe. Die BBSA legte dar, dass sie bei der Erfüllung ihrer gesetzlichen Aufgaben keine besonders schützenswerten Personendaten bearbeitet. Da sie nicht verhindern kann, dass Dritte E-Mails mit sensiblen Inhalten in Angelegenheiten, für die sie nicht zuständig ist, an sie senden, werden die Online-Postfächer täglich zweimal geleert. Unter diesen Umständen erachtete die DSA die Nutzung von Exchange-Online als zulässig.

Zeitwirtschaftssystem der Universität Bern ohne MS Azure

Die UniBE plante eine Umstellung ihres Zeitwirtschaftssystems auf die Lösung eines Lieferanten, die auf der Cloud-Lösung MS Azure basierte. Als privater Anbieter hatte der Lieferant die von ihm benutzten Services nach den allgemeinen Datenschutzbedingungen und ohne Zusatzvereinbarungen für die öffentliche Hand eingekauft. Diese Zusatzvereinbarungen – namentlich der Rahmenvertrag der Digitalen Verwaltung Schweiz – enthalten besondere Zusagen namentlich zum anwendbaren Recht und zum Gerichtsstand (Schweiz statt Irland) im Fall von Streitigkeiten. Damit die Auslagerung der Daten für die betroffenen Personen nicht nachteilig ist, musste der Lieferant entweder die gleichen Zusagen von Microsoft erhalten oder die Lösung mit anderen Ressourcen anbieten. Als Ergebnis erfolgte bei laufender Vorabkontrolle ein Technologiewechsel, und der Lieferant nutzte andere Ressourcen als jene von Microsoft.

Kohortenstudie «Bern, get ready» (BEready) der Universität Bern

Die DSA prüfte die datenschutzrechtliche Konformität der von der UniBE geplanten elektronischen Personendatenbearbeitung im Rahmen der Kohortenstudie BEready. Ziel der Studie ist es, die Bevölkerung des Kantons Bern abzubilden und wichtige Langzeitdaten zu sammeln, um das Wissen über bestehende Infektionskrankheiten und die Reaktionsbereitschaft auf neue Gesundheitsbedrohungen zu verbessern. BEready schliesst im gesamten Kanton Bern etwa 1 500 Haushalte ein, die aus Erwachsenen, Kindern und Haustieren bestehen. Weil die geplante Lösung teils auf MS Cloud-Services beruhte, verlangte die DSA unter anderem, dass die damit verbundenen Restrisiken – namentlich der Kontrollverlust gegenüber Microsoft – ausdrücklich ausgewiesen und von der zuständigen Institutsleitung akzeptiert werden.

ERP-System SAP: Auslagerung von Datenbearbeitungen in Cloud-Services

Die der DSA in einer ersten Etappe unterbreitete Einführung des neuen Enterprise Resource Planning (ERP-) Systems SAP zur Ablösung der Finanz- und Personalinformationssysteme FIS und PERSIKA beruhte ausschliesslich auf lokal betriebenen Komponenten. In der zweiten Etappe sollten bestimmte Services nicht mehr bei der Bedag betrieben, sondern aus der SAP-Cloud bezogen werden. Deshalb unterbreiteten einerseits die Finanzverwaltung (FV) ein übergreifendes Informationssicherheitskonzept und andererseits das Personalamt (PA) ein Datenschutzkonzept für erste Personalprozesse unter Einsatz von Cloud-Services zur Vorabkontrolle. Dabei ging es bisher nur um Bearbeitungen von nicht besonders schützenswerten Personendaten, wie es der Regierungsrat auch für die Einführung von M365 in der Kantonsverwaltung vorgegeben hatte. Personendaten mit erhöhtem Schutzbedarf können bis zum Nachweis von überzeugenden neuen technischen Lösungen (z. B. Verschlüsselungslösungen) nicht in der SAP-Cloud bearbeitet werden. Weil die SAP-Cloud-Services selbst auf einer MS Azure-Plattform betrieben werden, waren auch die sich daraus ergebenden Risiken zu prüfen. Für das vom PA vorgelegte Learning Management System zur Kursadministration für die interne Aus- und Weiterbildung der Mitarbeitenden konnte die Erfüllung der datenschutzrechtlichen Anforderungen dargelegt werden.

Einsatz von WhatsApp für Rekrutierungen

Das PA gelangte mit einem Vorschlag an die DSA, wonach Bewerbungen künftig auch per WhatsApp eingereicht werden können. Nach Ansicht der DSA kann WhatsApp für von Behörden verantwortete Datenbearbeitung nicht rechtmässig eingesetzt werden. Bei der Installation und Verwendung von WhatsApp werden einerseits sämtliche Kontaktdaten der nutzenden Person an Meta übermittelt, also auch von Personen, die WhatsApp nicht verwenden und der Datenübermittlung

nie zugestimmt haben. Andererseits werden die ebenfalls übermittelten Randdaten von Meta für eigene Zwecke (z. B. zum Vorschlagen von «Freunden» in anderen Social Media-Anwendungen) verwendet, was gegen das Zweckbindungsgebot verstösst. Sobald Behörden einen bestimmten Kommunikationskanal – hier zum Einreichen von Bewerbungen – anbieten, sind sie dafür verantwortlich, dass jener datenschutzkonform benützt werden kann. Sie dürfen Stellensuchende weder dazu verleiten, mit WhatsApp die Persönlichkeitsrechte Dritter zu verletzen, noch sollen sie aus bereits begangenen Datenschutzverletzungen einen Nutzen ziehen. Die DSA beurteilte deshalb die Verwendung von WhatsApp im Bewerbungsprozess als unzulässig. Dafür empfahl sie dem PA, Verbesserungen beim bestehenden digitalen Bewerbungsangebot zu prüfen.

Automatisierte Fahrzeugfahndung mit Durchfahrtenspeicherung

Seit einer Änderung des PolG per August 2024 darf die KAPO «zur Fahndung nach Personen oder Sachen sowie zur Erkennung, Verhinderung und Verfolgung von Verbrechen oder Vergehen» automatisiert erfasste Kontrollschilder von Fahrzeugen nicht mehr nur mit polizeilichen Datenbanken abgleichen und bei fehlender Übereinstimmung sofort wieder vernichten, vielmehr darf sie alle Daten bis zu 60 Tage aufbewahren und unter bestimmten Voraussetzungen auswerten (siehe zu den grundsätzlichen Vorbehalten der DSA den Jahresbericht 2022, S. 23 f.). Die neu mögliche Speicherung der Durchfahrten stellte eine wesentliche Änderung der bisherigen Datenbearbeitung dar und musste deshalb der DSA zur Vorabkontrolle unterbreitet werden. Deren Empfehlungen betrafen namentlich die ausführlichere Beschreibung der Datenvernichtung auf den von der Körperschaft Polizeitechnik und -informatik Schweiz (PTI) betriebenen Servern. Nachdem die KAPO die Empfehlungen der DSA befolgt hatte, erschien die Umsetzung des neuen Instruments als grundsätzlich datenschutzkonform. Allerdings stellte das Bundesgericht im Urteil vom Oktober 2024 zum luzernischen Polizeigesetz fest, dass die Gesetzgebungskompetenz im Bereich der Strafverfolgung ausschliesslich beim Bund liege und deshalb die kantonale Regelung einer automatisierten Fahrzeugfahndung (AFV) zum primären Zweck der Strafverfolgung unzulässig sei (Urteil 1C_63/2023, E. 3.5). Nach dem bernischen PolG soll die AFV auch für die präventive Polizeiarbeit zum Einsatz kommen. Gegen die betreffende Regelung im PolG ist ebenfalls Beschwerde an das Bundesgericht erhoben worden, das darüber entscheiden wird, inwieweit die AFV und insbesondere die umfangreiche Vorratsdatenbeschaffung im Rahmen der Durchfahrtenspeicherung allein für präventive Zwecke verhältnismässig ist.

Elektronische Geschäftsverwaltung der Fachstelle Datenschutz der Stadt Bern

Die Fachstelle Datenschutz (FADS) ist die kommunale Aufsichtsstelle der Stadt Bern. Sie und die städtische Ombudsstelle planten die Einführung einer neuen

elektronischen Geschäftsverwaltung, in der auch besonders schützenswerte Personendaten bearbeitet werden und die daher von Gesetzes wegen der Pflicht zur Vorabkontrolle unterlag. Allerdings konnte die für kommunale Vorabkontrollen zuständige FADS die eigene Datenbearbeitung nicht vorabkontrollieren. Sie fragte deshalb die DSA an, ob diese die Vorabkontrolle durchführen würde. Das KDSG sieht vor, dass die DSA die Oberaufsicht über die kommunalen Aufsichtsstellen ausübt. Zudem soll sie mit den anderen Aufsichtsstellen im Kanton zusammenarbeiten, und sie darf in anderen Gemeinwesen Aufgaben der Datenschutzaufsicht wahrnehmen, soweit dies vereinbart ist. Auf dieser Grundlage war die DSA bereit, die Vorabkontrolle durchzuführen. Ihre Empfehlungen zu den erwartungsgemäss sauber aufbereiteten Unterlagen betrafen vor allem Fragen der technischen Dokumentation, namentlich zur Trennung der Daten von mehreren Kunden beim gleichen Hoster. Alle Empfehlungen wurden von der FADS umgesetzt.

6.3.2. Videoüberwachungen

Seit 2020 gilt das totalrevidierte PolG mit teilweise neuen Bestimmungen zu Videoüberwachungen. Während die materiellen Anforderungen an Videoüberwachungen weitgehend unverändert aus dem früheren Recht übernommen wurden, ist für Überwachungen zum Schutz öffentlicher Gebäude keine Zustimmung der KAPO mehr nötig. Diese ist jedoch weiterhin in einem Rückspracheverfahren zu konsultieren, wobei die KAPO das Ergebnis der Vorabkontrolle der zuständigen Datenschutzaufsichtsstelle – für kantonale Behörden der DSA – berücksichtigt. Zu den Anforderungen an die Informationssicherheit und den Datenschutz erarbeitete die DSA eine Checkliste, welche die KAPO auf ihrer Webseite als Hilfsmittel zur Verfügung stellt.

Auch ohne explizite gesetzliche Grundlage werden geeignet ausgestaltete Videoüberwachungen als zulässig erachtet, wenn sie zur Erfüllung von gesetzlichen Aufgaben notwendig sind (z. B. die Echtzeitüberwachung von frisch operierten Patientinnen und Patienten in der Aufwachstation eines Spitals).

Grundschutz der Videoüberwachungs-Infrastruktur am Inselspital

In den Vorjahren hatte die Insel Gruppe AG mehrere Videoüberwachungen an verschiedenen Orten – unter anderem im neuen Anna Seiler-Haus – zur Vorabkontrolle unterbreitet, nicht jedoch den Grundschutz der gesamten Videoüberwachungs-Infrastruktur. Die durchgeführte Prüfung war deshalb nicht eine echte Vorabkontrolle, da die Infrastruktur bereits in Betrieb war. Vielmehr ging es darum, eine Grundlage für spätere Vorabkontrollverfahren im Videoüberwachungsbereich zu schaffen: Künftig sollte es möglich sein, auf der geprüften Infrastruktur aufzubauen und die Kontrollen nur für Änderungen an der Infrastruktur oder bei den Kameras durchzuführen. Die Videoüberwachungs-Infrastruktur eines Spitals muss

die Anforderungen an den erhöhten Schutzbedarf von Patientendaten erfüllen, die besonders schützenswerte Personendaten sind und unter dem Schutz besonderer Geheimhaltungspflichten stehen. Im Rahmen der dokumentenbasierten Prüfung konnten nicht alle Aspekte abschliessend kontrolliert werden, weil die Verantwortlichen des Inselspitals teilweise auf Unterlagen verwiesen, die für das Audit des allgemeinen ICT-Grundschutzes von 2021/22 eingereicht worden waren. Die Videoüberwachungs-Infrastruktur und ihre spezifischen Komponenten wie das zugehörige Netzwerk, die Server, die mobilen Clients und die Verschlüsselung waren jedoch nicht Gegenstand jenes Audits, weshalb der Soll-Zustand insoweit nicht geprüft werden konnte. Die Komponenten werden im Rahmen eines nächsten Audits kontrolliert werden müssen.

Videoüberwachung der Gemeinde Saanen

Die kommunale Aufsichtsstelle der Gemeinde Saanen bat die DSA um Beratung bei deren Vorabkontrolle eines Vorhabens der Gemeinde: Diese beabsichtigte, die zentralen Talein- und -ausfahrten mit Rundumsicht- und Fahrzeugschilderkennungskameras überwachen, um das allgemeine Sicherheitsgefühl der Bevölkerung zu stärken und die Polizeibehörden bei der Fahndung nach Straftätern zu unterstützen. Die DSA teilte die Ansicht der kommunalen Aufsichtsstelle, dass die Videoüberwachung offensichtlich nicht zulässig war. Das Vorhaben war nicht nur unverhältnismässig, sondern es fehlte bereits eine Rechtsgrundlage dafür. Das PolG erlaubt Videoüberwachungen nur an konkreten Orten, an denen Straftaten begangen worden sind oder mit solchen zu rechnen ist (sog. «Gefahren- bzw. Kriminalitätsschwerpunkte»). Verkehrsachsen und Kreuzungen per se sind ebenso wenig solche Orte wie das gesamte Gemeindegebiet. Eine so weitgehende Videoüberwachung läge nahe bei einer Verletzung des Kerngehalts des Grundrechts auf Datenschutz.

Videoüberwachung einer kommunalen Abfallsammelstelle

Eine Gemeinde erkundigte sich bei der DSA nach der Möglichkeit der Überwachung einer Abfallsammelstelle, an der regelmässig unzulässiger Abfall deponiert wurde. Eine solche Überwachung setzt voraus, dass das Verhalten eine Straftat darstellt, die verhindert oder geahndet werden soll. Das schweizerische Strafgesetzbuch erlaubt es den Kantonen, zusätzliche Strafbestimmungen zu erlassen, die bestimmte Verhaltensweisen mit Busse bestrafen. Das bernische Gemeindegesetz wiederum sieht die Möglichkeit vor, dass Gemeinden in ihren Reglementen Widerhandlungen mit Busse bestrafen. Davon hatte die betreffende Gemeinde in ihrem Abfallreglement Gebrauch gemacht. Daher war auf dieser Grundlage eine Videoüberwachung nach PolG grundsätzlich möglich. Für die Durchführung der Vorabkontrolle verwies die DSA die Gemeinde an ihre kommunale Aufsichtsstelle.

6.4 Audits

Im Rahmen ihres gesetzlichen Auftrags, die Anwendung der Vorschriften über die Informationssicherheit und den Datenschutz (ISDS) kontinuierlich zu überwachen, führte die DSA im Berichtsjahr acht ISDS-Audits durch, wobei einerseits wesentliche Fachapplikationen der Verwaltung und andererseits der Gesundheitsbereich im Fokus der risikoorientierten DSA-Planung standen. Dort wurden primär der ICT-Grundschutz und die Medizintechnik-Infrastruktur – also Geräte, die bei der Behandlung und Diagnose eingesetzt werden – geprüft. Weiter begleitete und überwachte die DSA die Umsetzung von ISDS-Massnahmen aus den in den Vorjahren durchgeführten Audits. Die kontinuierliche Begleitung der Folgearbeiten zu ihren Audits ermöglicht es der DSA, den Überblick längerfristig zu behalten.

Für die DSA ist es in einem Umfeld mit einer sehr hohen Veränderungstendenz (u. a. durch die Digitalisierungsvorhaben) wesentlich zu verstehen, welche Herausforderungen die geprüften Stellen zu bewältigen haben. Durch eine frühe Kontaktaufnahme und Begleitung durch die DSA kann eine qualifizierte und sachdienliche ISDS-Beurteilung erfolgen. ISDS-Anforderungen werden teilweise immer noch als «Hindernisse» angesehen. Diese Sichtweise greift zu kurz, denn diese Anforderungen leisten einen wesentlichen Beitrag zur Erkennung und Minderung von Risiken bei der elektronischen Datenbearbeitung. Die kantonalen digitalen Angebote könnten ohne wirksame ISDS-Massnahmen bösartigen Angriffen nicht standhalten. Die Folgen wären ein Daten- und damit einhergehend ein grosser Vertrauensverlust. Die proaktive und risikoorientierte Vorgehensweise trägt daher zum Vertrauen bei der Nutzung der zunehmend digitalisierten kantonalen Angebote durch die Bürgerinnen und Bürger bei.

Allgemeine Erkenntnisse

Neben ersichtlichen Verbesserungen musste im Berichtsjahr wiederholt festgestellt werden, dass erforderliche ISDS-Aufgaben und -Massnahmen teilweise nicht mit der gebotenen Sorgfalt wahrgenommen bzw. umgesetzt wurden. Die Gründe dazu sind vielfältig; so können das Tagesgeschäft und Projekte die für die Umsetzung von ISDS-Massnahmen notwendigen Ressourcen binden. Auch fehlte es teilweise an einer wirksamen Steuerung (Governance) der ISDS-Anforderungen. Für eine solche Steuerung müssen mess- und überprüfbare Vorgaben bestehen. Eine institutionalisierte Governance steuert systematisch die Summe aller ISDS-Anforderungen und -Massnahmen. Dies war nicht immer erkennbar.

Bei den Spitälern zeigte sich, wie bereits in den letzten Berichtsjahren, dass der Betrieb der Medizintechnik-Infrastruktur stark von den Lieferanten abhängig ist. Die Spitäler haben hier einen eingeschränkten Einfluss auf die Betriebssicherheit und den Datenschutz. Eine ganzheitliche Sicht auf die kritischen Medizintechnik-Geräte fehlte teilweise. Dabei ist es wesentlich zu verstehen, dass bei der

Evaluation, Beschaffung, Betrieb und Ausserbetriebnahme der Geräte eine systematische Sicherstellung der ISDS-Anforderungen durch das verantwortliche Spital zu gewährleisten ist.

Wie schon in den letzten Jahren festgestellt, übertragen die verantwortlichen Behörden zunehmend ISDS-Aufgaben an externe Dienstleister und Lieferanten (Lieferkette). Dies steht auch im Zusammenhang mit der Digitalisierung und der zunehmenden Nutzung von Cloud-Lösungen und -Services. Grundsätzlich befinden sich externe Lieferketten nicht im Einfluss- und Kontrollbereich der verantwortlichen Behörden. Die nachweisbare ISDS-Steuerung und -Überwachung der Lieferketten war nicht durchgehend erkennbar.

Eine weitere Feststellung betrifft das Projektmanagement. Die DSA erkannte bei ihren Audits wiederholt, dass die Projektverantwortlichen ihre ISDS-Aufgaben bei der Einführung von neuen Fachanwendungen nicht vollständig wahrnehmen. Es fehlte teilweise an einer nachvollziehbaren Übergabe der vorgegebenen ISDS-Ergebnisse (ISDS-Soll) aus dem Projekt an den Betrieb (Projektabschluss zu Betriebsaufnahme). Dies führte dazu, dass ISDS-Anforderungen und die dazugehörenden wesentlichen Dokumente nicht vollständig geprüft und abgenommen und in der Folge nur teilweise an den Betrieb übergeben wurden. Diesen Mangel gilt es im Rahmen des Projektmanagements noch zu verbessern.

ICT-Grundschutz des Spitals Privatklinik Linde AG

Die DSA prüfte beim Spital Privatklinik Linde AG, einer Klinik der Hirslanden-Gruppe, die Erfüllung der ISDS-Anforderungen an die ICT-Infrastruktur in Bezug auf den Grundschutz (Normen, Rahmenwerke, Organisation, Prozesse und Kontrollen). Hierfür wurden ausgewählte Kontrollen der Prüfbereiche «ISDS-Governance», «ISDS-Konzept(e) und Schutzmassnahmen», «Prozesse des Benutzermanagements», «Datenspeicherung», «Netzwerksicherheit», «Client und Server Sicherheit», «Change- und Release-Management», «Outsourcing» sowie «physische Sicherheit der Rechenzentren» geprüft. Die ICT der Privatklinik Linde AG wurde in den vergangenen Jahren nahezu vollständig in die zentrale technische ICT-Infrastruktur der Hirslanden-Gruppe integriert.

In allen geprüften Bereichen ergaben sich Feststellungen, die mehrheitlich als mittlere und hohe Risiken eingestuft wurden. Dabei wurden unklare Zuständigkeiten, fehlende aktuelle und durch das Management autorisierte ISDS-Handlungsanweisungen als auch die teilweise nicht vollständige Dokumentation sowie technische Defizite erkannt. Kontrollen und die Gesamtübersicht im Bereich der Lieferantenketten sind ebenso noch zu verbessern. Auch im Bereich des Kontinuitätsmanagements ergaben sich Feststellungen. Trotz einer hohen technischen Komplexität und einer starken Auslastung der involvierten Mitarbeiter im Tages- sowie Projektgeschäft konnte die DSA ihre Aufgabe in einem angenehmen und transparenten Rahmen wahrnehmen.

Fachanwendung SUSA des Strassenverkehrs- und Schifffahrtsamts

Beim Strassenverkehrs- und Schifffahrtsamt des Kanton Berns (SVSA) wurden die Erfüllung der ISDS-Anforderungen, die ICT-Prozesse sowie die ISDS-Kontrollen rund um die Kernanwendung SUSA geprüft. Hierfür wurden ausgewählte Prüfbereiche wie das «Outsourcing», «ISDS-Governance», «ISDS-Konzept(e) und Schutzmassnahmen», «Change- und Release Management», sowie «Prozesse des Benutzermanagements (IAM)» eingehender untersucht.

Das Gesamtergebnis der Prüfung ergab Feststellungen, die im tieferen und mittleren Risikobereich zu liegen kamen. Insbesondere bei den ISDS-Kontrollen der Lieferanten und im Bereich der Steuerung des Risikomanagements als auch bei der Sensibilisierung der Mitarbeitenden bestehen noch Verbesserungsmöglichkeiten. Die Prüfungshandlungen konnten dank der aktiven und zuvorkommenden Mithilfe der SVSA-Mitarbeitenden effizient durchgeführt werden.

Medizintechnik-Infrastruktur der Spitäler FMI

Bei den Spitälern FMI wurde die ICT-Medizintechnik-Infrastruktur auf Einhaltung des Grundschutzes in Bezug auf die internen ISDS-Vorgaben und -Weisungen (organisatorisch, technisch und prozessual), Normen und Rahmenwerke sowie den implementierten ISDS-Massnahmen (Prozesse, Kontrollen, Organisation) geprüft. Die Prüfung erfolgte primär risikobasiert in den Prüfbereichen «ISDS-Governance», «ISDS-Konzept(e) und Schutzmassnahmen», «Prozesse des Benutzermanagements», «Change- und Release-Management», sowie «Outsourcing».

In allen Prüfbereichen ergaben sich Feststellungen mehrheitlich im mittleren und hohen Risikobereich. Insbesondere fehlen autorisierte ISDS-Weisungen. Diese sind zum Zeitpunkt der Prüfungshandlungen noch nicht freigegeben und umgesetzt. Weiter fehlt eine konsolidierte Gesamtübersicht, die alle bestehenden Medizintechnik-Geräte zusammenfassend abbildet und überwacht. Ein nachvollziehbares Risikomanagement über die Lieferketten und den Betrieb der Medizintechnik-Infrastruktur ist nicht vollumfänglich ersichtlich. Im Bereich des Kontinuitätsmanagement sind die notwendigen konzeptionellen Vorgaben und ein Test in Arbeit. Die DSA konnte ihre Prüfung in einem konstruktiven sowie freundlichem Umfeld durchführen.

Konzernanwendung Umantis des Personalamts

Die Erfüllung der ISDS-Anforderungen bei der Konzernanwendung Umantis wurde im PA geprüft. Umantis unterstützt einheitlich die gesamte kantonale Personalrekrutierung mit einem durchgehenden digitalen Aufgabenprozess. Die Prüfgebiete umfassten die «ISDS-Governance», «ISDS-Konzept(e) und Schutzmassnahmen», «Prozesse des Betriebs» und das «Identity and Access Management» (IAM),

«Outsourcing» und «Leistungsverträge», «Datenhaltung und die Schnittstellen» sowie zusammengefasst das «Kontinuitäts- und Notfallmanagement».

Im Rahmen der durchgeführten Prüfung wurden in allen Prüfbereichen Feststellungen mit einem mittleren und teils höheren Risiko gemacht. Insbesondere bei den Kontrollen der Lieferanten sowie der Aktualisierung der Dokumentation als auch beim Kontinuitätsmanagement sind Verbesserungen angebracht. Das Prüfergebnis konnte durch die gute Unterstützung der PA-Mitarbeitenden in einem zuvorkommenden und versierten Umfeld erreicht werden.

SAP Kanton Bern der Finanzverwaltung

Die FV führt das *Customer Center of Expertise* (CCoE) für die SAP-Systeme der Kantonsverwaltung. Für diese Systeme wurde die Erfüllung der ISDS-Anforderungen betreffend Organisation, Prozesse und Kontrollen namentlich im Bereich «Prozesse des Benutzermanagements» (IAM) geprüft. Angesichts der kritischen Berechtigungen im SAP-Basis-Umfeld wurde der sog. Parameter «SE06» zur Systemänderbarkeit dezidiert geprüft.

Die Prüfung ergab Risiken im mittleren als auch im hohen Bereich. Teilweise konnte nachvollzogen werden, dass es sich bei den Prüfergebnissen um Restanzen aus dem SAP-Einführungsprojekt der vergangenen Jahre handelte. Hierbei sind insoweit Verbesserungen notwendig, als dass bei der Abnahme der produktiven SAP-Systeme für den ordentlichen Betrieb keine rein projektspezifischen Rollen und Rechte in der produktiven Umgebung akzeptiert werden sollten. Die Prüfung erfolgte auf der Basis einer sehr guten und konstruktiven Zusammenarbeit zwischen den verantwortlichen CCoE-Mitarbeitenden der FV und der DSA.

ICT-Grundschutz der Universität Bern

Bei den zentralen Informatikdiensten der UniBE wurde die Erfüllung der ISDS-Anforderungen an die ICT-Infrastruktur in Bezug auf den Grundschutz (Normen und Rahmenwerke, Organisation, Prozesse und Kontrollen) geprüft. Hierfür wurden die Prüfbereiche «ISDS-Governance», «ISDS-Konzept(e) und Schutzmassnahmen», «Prozesse des Benutzermanagements (IAM)», «Datenspeicherung», «Netzwerksicherheit», «Client- und Server-Sicherheit», «Outsourcing» sowie «Physische Sicherheit der Rechenzentren» der zentralen Prozesse ausgewählt.

In allen Prüfbereichen wurden Risiken im mittleren und hohen Risikobereich erkannt. Die Institute der UniBE gestalten ihre ICT-Infrastruktur grösstenteils eigenständig, ohne dass die zentralen Informatikdienste der UniBE direkten Weisungseinfluss darauf haben, weshalb die ISDS-Vorgaben, Prozesse, Systeme, Netzwerke und Anwendungen für die gesamte UniBE ICT unterschiedlich und auch unvollständig abgestimmt sind. Dies erhöht die ICT-Risiken der UniBE

insgesamt. Es drängen sich daher auch organisatorische und strukturelle Verbesserung auf. Die Prüfung profitierte von einem konstruktiv freundlichen Umfeld und einer klar ersichtlichen Bereitschaft zur Unterstützung der DSA bei der Ausübung ihrer Tätigkeit.

Fachanwendung Evidence der Regierungsstatthalterämter

Die Fachanwendung Evidence wird bei den Regierungsstatthalterämtern zur elektronischen Verwaltung der Geschäftsfälle eingesetzt. Stellvertretend wurde Evidence beim RSTA Bern-Mittelland geprüft. Die Prüfgebiete umfassten die «ISDS-Governance», die «ISDS-Konzept(e) und Schutzmassnahmen», «Prozesse des Betriebs» und das «Identity and Access Management» (IAM), «Outsourcing» und «Leistungsverträge», «Datenhaltung und die Schnittstellen» und zusammengefasst das «Kontinuitäts- und Notfallmanagement».

Die DSA machte in allen Prüfbereichen Feststellungen im mittleren und auch hohen Risikobereich. Dabei zeigten sich Defizite im Bereich der ICT-Governance, der Dokumentation (Vollständigkeit und Aktualität), der ISDS-Kontrollen und dem Kontinuitätsmanagement. Die erkannten Defizite in diesen Bereichen müssen in der Folge mit entsprechenden Massnahmen verbessert werden. Die fachlich versierten und freundlichen Mitarbeitenden des RSTA und des Digital Managements der DIJ leisteten einen massgebenden Beitrag zum Gelingen dieser Prüfung.

ICT-Grundschutz der Spitex Bern

Bei der Spitex Bern wurde die Erfüllung der ISDS-Anforderungen im Bereich des ICT-Grundschutzes in Bezug auf die internen ISDS-Vorgaben und -Weisungen (organisatorisch, technisch und prozessual), Normen und Rahmenwerke und die bereits implementierten Massnahmen (Organisation, Prozesse, Kontrollen) geprüft. Hierfür wurden die Prüfbereiche «ISDS-Governance», «ISDS-Konzept(e) und Schutzmassnahmen», «Prozesse des Benutzermanagements», «Datenspeicherung», «Netzwerksicherheit», «Client und Server Sicherheit», «Change- und Release-Management», «Outsourcing» sowie «physische Sicherheit der Rechenzentren» eingehender untersucht.

Das Prüferergebnis umfasste mehrheitlich Risiken im mittleren und höheren Bereich. Die Spitex Bern bezieht ihre ICT-Services grösstenteils bei externen Lieferanten und Dienstleistern. Dieses Vorgehen entspricht einem gängigen Modell, da die Bereitstellung von ICT-Services nicht zum Kerngeschäft der Spitex Bern gehört. Die typischen Risiken dieses Outsourcing-Modells umfassen i. d. R. die fehlenden Kontrollen und die verminderte Transparenz z. B. in Bezug auf die Sicherheit und Aktualität der zur Verfügung gestellten ICT-Infrastruktur. Zudem ist ein hohes Mass an Vertrauen notwendig, da sich das technische Fachwissen

mehrheitlich extern befindet. Die Prüfung fand in einem beispielhaft freundlichen und offenen sowie hilfsbereiten Umfeld satt.

6.5 Weitere aufsichtsrechtliche Instrumente

6.5.1. Bearbeitung von Meldungen über Datenschutzvorfälle

Gestützt auf die Einführungsverordnung zur EU-Datenschutzrichtlinie (EV EDS) besteht im Kanton Bern vorerst nur im Polizei- und Strafbereich eine Pflicht, Vorfälle im Bereich der Datensicherheit – die ungewollte Vernichtung, Veränderung oder Offenbarung von Daten an Unbefugte – an die zuständige Datenschutzaufsichtsstelle zu melden. Mit der Totalrevision des KDSG soll diese Pflicht auf alle öffentlichen Aufgaben ausgedehnt werden. Die DSA empfiehlt allerdings bereits heute allen Behörden, Datenschutzvorfälle an sie zu melden, damit die zu treffenden Massnahmen, zu denen in bestimmten Fällen die Information betroffenen Personen gehört, gemeinsam abgestimmt werden können.

Im Berichtsjahr wurden der DSA zehn Datenschutzvorfälle gemeldet, wovon einer in den Anwendungsbereich der EV EDS fiel (Fehlzustellung einer gerichtlichen Vorladung durch die Post). Die anderen Vorfälle betrafen unter anderem die Entwendung des Notebooks einer Betreuerin durch Klienten einer heilpädagogischen Institution, die Veröffentlichung eines Patientendossiers in einer WhatsApp-Gruppe, den ungeschützten Zugang zu einer grossen Anzahl Personalien der Absolventinnen und Absolventen von Studiengängen einer Bildungsinstitution über das Internet, die Benutzung eines Online-Konvertierungstools zum Umwandlung einer Datei mit den Namen aller Klientinnen und Klienten einer in einem sensiblen Bereich tätigen Behörde sowie den Zugang zum Kundenkonto der vorbenützenden Person bei einer Behörde, wenn mehrere Personen hintereinander das gleiche Gerät benutzten.

6.5.2. Begründete Anträge und Beschwerdeverfahren

Das Gesetz sieht vor, dass die DSA bei festgestellten Rechtsverstössen oder Mängeln deren Beseitigung in Form eines mit einer Begründung versehenen Antrags empfiehlt; will die verantwortliche Behörde dem Antrag der DSA nicht oder nur teilweise stattgeben, erlässt sie eine entsprechende Verfügung, welche die DSA bei der zuständigen Direktion bzw. beim Verwaltungsgericht anfechten kann (Art. 35 Abs. 3 bis 5 KDSG). In der Praxis spricht die DSA ihre Empfehlungen

– namentlich nach aufsichtsrechtlichen Rückfragen, bei Vorabkontrollen und Audits – nicht als formelle Anträge in diesem Sinne aus, weil die verantwortlichen Behörden fachlich nachvollziehbare Empfehlungen regelmässig 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, müsste die DSA den formellen Weg beschreiten.

Im Berichtsjahr erliess die DSA keinen formellen Antrag und führte keine Beschwerde gegen die ablehnende Verfügung einer verantwortlichen Behörde.

6.5.3. Oberaufsicht über die Aufsichtsstellen der Gemeinden

Das geltende Datenschutzgesetz sieht vor, dass die Gemeinden und anderen gemeinderechtlichen Körperschaften sowie die Landeskirchen und ihre regionalen Einheiten für ihren Bereich eine eigene Aufsichtsstelle bezeichnen (Art. 33 KDSG); die DSA übt die Oberaufsicht aus und ist Anlaufstelle für die kommunalen Aufsichtsstellen.

Um die verlangte Unabhängigkeit gewährleisten zu können, haben die Gemeinden verschiedene Lösungen gewählt: Kleine und mittlere Gemeinden haben regelmässig ihr Rechnungsprüfungsorgan als Aufsichtsstelle bezeichnet, in Gemeinden mit einem Parlament nimmt oftmals die Geschäftsprüfungskommission die Aufgaben der Datenschutzbehörde wahr. Einige Gemeinden haben eine fachkundige Anwaltskanzlei als Aufsichtsstelle mandatiert, einzig die Stadt Bern verfügt über eine dedizierte Datenschutz-Aufsichtsstelle.

Entsprechend heterogen sind die ISDS-Kenntnisse der kommunalen Aufsichtsstellen sowie Umfang und Qualität der Beratung, welche diese ihren Gemeindebehörden anbieten können. Deshalb soll im Rahmen der laufenden Totalrevision des KDSG die Datenschutzberatung und -aufsicht für die meisten Gemeinden an die DSA übertragen werden. Bis dahin erteilt die DSA den Gemeindebehörden Auskünfte jeweils mit dem Vorbehalt ihrer fehlenden Zuständigkeit (und unter Hinweis auf die zuständige kommunale Aufsichtsstelle) sowie mangels dafür vorgesehener personeller Ressourcen nur in sehr beschränktem Umfang (siehe Ziff. 6.3.2. zu den kommunalen Videoüberwachungen).

6.6 Interkantonale Zusammenarbeit

Präsidium und Vorstand von privatim

Seit November 2020 hat der Datenschutzbeauftragte das Amt des Präsidenten der Konferenz der schweizerischen Datenschutzbeauftragten «privatim» inne. Diese führte im Berichtsjahr zwei Plenumsversammlungen durch und beleuchtete im Fachteil zum Frühjahrsplenum die Rechtsfolgen von Datenschutzverletzungen aus der Sicht des Datenschutzrechts, des Informationssicherheitsgesetzes des Bundes, der Staatshaftung und des Strafrechts. Privatim verfasste insgesamt 11 Stellungnahmen im Rahmen von Vernehmlassungen des Bundes bzw. der KKJDP und stellte diese ihren Mitgliedern teils als Vorlage für deren Eingaben im jeweiligen Kanton zur Verfügung. In zahlreichen Kontakten mit kantonsübergreifend tätigen Organisationen – namentlich der Digitalen Verwaltung Schweiz, der Fachagentur Educa, der Schweizerischen Berufsbildungsämter-Konferenz, der Arbeitsgruppe Recht im Justizvollzug der KKJPD und der PTI – leistete privatim Beratungen zur datenschutzkonformen Umsetzung der jeweiligen Vorhaben. Erneut stand privatim in regelmässigem Austausch mit dem EDÖB, namentlich um sich in der Vernehmlassung zum POLAP-Konkordat abzustimmen (siehe Ziff. 6.2) und zusammen mit dem Bundesamt für Justiz eine Vereinfachung der Regelung zum anwendbaren Datenschutzrecht und der Aufsichtszuständigkeit während der Pilotphase zur Einführung der Plattform justitia.swiss für den elektronischen Rechtsverkehr in ersten Kantonen zu erreichen.

Arbeitsgruppen von privatim

Die *Arbeitsgruppe Digitale Verwaltung* traf sich drei Mal und befasste sich dabei namentlich mit dem Projekt Justitia 4.0 zur Einführung des elektronischen Rechtsverkehrs und mit dem CH-US Datenschutzrahmen bzw. dem zugehörigen Angemessenheitsbeschluss des Bundesrates.

Die *Arbeitsgruppe Sicherheit* begleitete die Arbeiten des Vereins Electronic Monitoring zur Erneuerung des gesamtschweizerischen Systems zur elektronischen Überwachung u. a. im Strafvollzug und unterzog dessen Dokumentation über den Datenschutz und die Informationssicherheit mehreren Reviews. Ferner prüfte die Arbeitsgruppe den Entwurf für eine Auftragsbearbeitungsvereinbarung zwischen der PTI und einem IT-Leistungserbringer im Rahmen des kantonsübergreifenden Vorhabens «Integriertes Lagebild 4.0» und bereitete für den Vorstand von privatim die Stellungnahme in der Vernehmlassung zum POLAP-Konkordat vor.

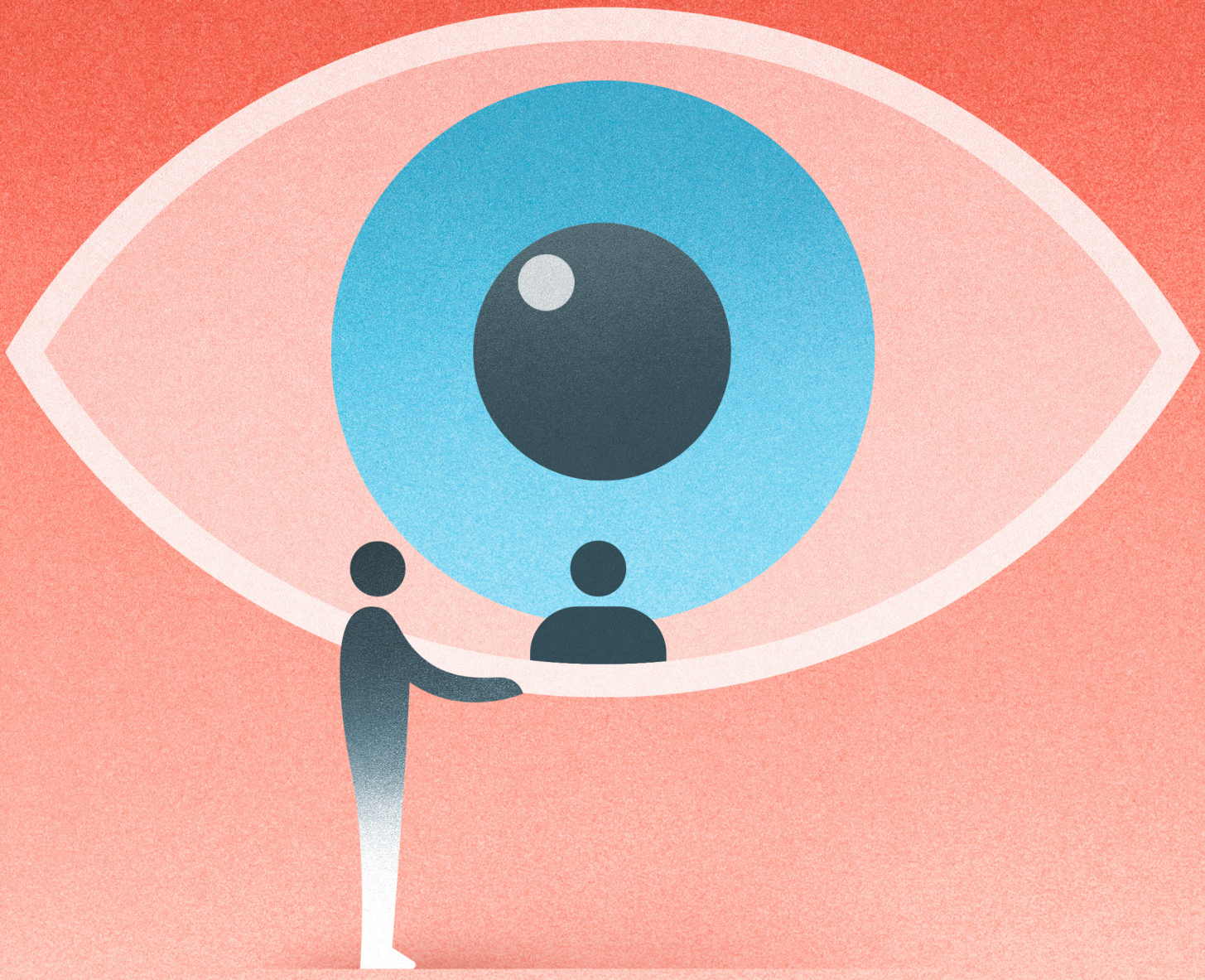
Die Mitglieder der *Arbeitsgruppe Gesundheit* trafen sich im Berichtsjahr unter der Leitung der stellvertretenden Datenschutzbeauftragten Recht zweimal virtuell und einmal vor Ort. Die Gruppe pflegt einen regen Erfahrungsaustausch zu aktuellen

Fragestellungen, welche die Datenschutzbehörden mehrerer oder aller Kantone und den Bund betreffen (können). Gestützt auf die Abklärungen der DSA zum Datenfluss zwischen dem kantonalen pharmazeutischen Dienst und Apotheken zur Bekämpfung von Rezeptfälschungen (siehe Ziff. 6.1.1) erhielten die Mitglieder Hinweise, um die Rechtsgrundlagen und die gelebte Praxis in ihrem Aufsichtsbereich zu überprüfen. Daneben beschloss die Gruppe, sich gezielte Basiswissen anzueignen, um für künftige neue Fragestellungen bereit zu sein. So organisierte sie zwei Inputreferate zum Thema Künstliche Intelligenz im Gesundheitsbereich.

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

7 Antrag

Kenntnisnahme.



8 Glossar / Abkürzungen

Abs.	Absatz
AFV	Automatisierte Fahrzeugfahndung
AG	Aktiengesellschaft
AHV	Alters- und Hinterlassenenversicherung
AKB	Ausgleichskasse des Kantons Bern
Art.	Artikel
AUE	Amt für Umwelt und Energie
BBSA	Bernische BVG- und Stiftungsaufsicht
CHF	Schweizer Franken
CCoE	Customer Center of Expertise SAP Kanton Bern
DIJ	Direktion für Inneres und Justiz
DSA	Datenschutzaufsichtsstelle des Kantons Bern
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
E.	Erwägung
eBau	Fachapplikation für das elektronische Baubewilligungsverfahren
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EU	Europäische Union
EV EDS	Einführungsverordnung zur EU-Datenschutzrichtlinie
f.	und folgende (Seite)
FADS	Fachstelle Datenschutz der Stadt Bern
FIN	Finanzdirektion
FV	Finanzverwaltung
GERES	Gemeinderegistersystem
GSI	Gesundheits-, Sozial- und Integrationsdirektion

GVB	Gebäudeversicherung Bern
ICT	Informations- und Telekommunikationstechnik
IMG	Gesetz über die Information und die Medienförderung
ISDS	Informationssicherheit und Datenschutz
I-SIVE	Informationssicherheitsverantwortliche(r)
IT	Informatik
KAIO	Amt für Informatik und Organisation
KAPO	Kantonspolizei
KDSG	(Kantonales) Datenschutzgesetz
KI	Künstliche Intelligenz
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
M365	Microsoft 365
MS	Microsoft
NAV	Verordnung über Niederlassung und Aufenthalt der Schweizerinnen und Schweizer
NFFS	Neues Fallführungssystem
PA	Personalamt
POLAP	Nationale Abfrageplattform für Polizeidaten
PolG	Polizeigesetz
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
PTI	Körperschaft Polizeitechnik und -informatik Schweiz
RSTA	Regierungsstatthalteramt
S.	Seite
sog.	sogenannte(r)
STA	Staatskanzlei

SVSA	Strassenverkehrs- und Schifffahrtsamt
TCHF	Tausend Schweizer Franken
u. a.	unter anderem
UniBE	Universität Bern
USA	Vereinigte Staaten von Amerika
WEU	Wirtschafts-, Energie- und Umweltdirektion
z. B.	zum Beispiel
Ziff.	Ziffer
ZMK	Zahnmedizinische Kliniken der UniBE
ZPV	Zentrale Personenverwaltung

Datenschutzaufsichtsstelle
des Kantons Bern

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

www.be.ch/dsa