Kanton Bern
Canton de Berne

Jahresbericht Datenschutzaufsichtsstelle 2023

Datenschutzaufsichtsstelle

Februar 2024

Impressum

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

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

Inhaltsverzeichnis

1 Vorwort

Im Jahr 1974 – also vor genau 50 Jahren – sang der deutsche Liedermacher Reinhard Mey den Text «Über den Wolken muss die Freiheit wohl grenzenlos sein». Was damals noch wörtlich zu verstehen war, wirkt heute unvermindert – wenn auch im übertragenen Sinn – als grosse Versuchung bei der digitalen Transformation der Verwaltung. Die Auslagerung von Datenbearbeitungen in die «Cloud» verspricht neue Möglichkeiten, welche vorher nicht denkbar oder mindestens nicht bezahlbar waren. Namentlich internationale Cloud-Infrastrukturen, die potentiell allen Internet-Nutzenden zur Verfügung stehen (sog. «Public Cloud»), erlauben Skaleneffekte durch die dynamische Zuweisung von Rechen- und Speicherleistungen nach dem jeweiligen Bedarf der Kunden, womit sich Investitionskosten senken lassen. Gleichzeitig führt die Übermittlung von Personendaten in eine für die verantwortlichen Behörden weitgehend unbekannte Infrastruktur zu Abhängigkeiten und Kontrollverlusten beim Schutz von Grundrechten.

Im Berichtsjahr wurde die kantonale Datenschutzaufsichtsstelle (DSA) deshalb mit zahlreichen Geschäften sowohl aus der Kantonsverwaltung wie auch von dezentralen Aufgabenträgern zu Cloud-Nutzungen befasst. Ein wiederkehrendes Thema war und ist die Einführung von Diensten aus der Produktepalette von Microsoft 365 (M365). Dem Regierungsrat wurden die Restrisiken bei der geplanten Nutzung von M365 in der Kantonsverwaltung zur Kenntnis gebracht und von diesem akzeptiert; die Vorabkontrolle der zugehörigen Massnahmen zum Schutz der Grundrechte war Ende 2023 noch nicht abgeschlossen. Auch die Universität Bern und die Insel Gruppe AG legten der DSA Pläne zur Einführung von M365 vor. Dass der Kontrollverlust bei in der Schweiz angebotenen Online-Diensten sehr viel geringer ist, zeigte die Prüfung der Plattform E-Mitwirkung, wo die Empfehlungen der DSA bewirkten, dass der Anbieter technische und organisatorische Änderungen an seinem Dienst vornahm.

Als neues Thema für den Datenschutz trat die Nutzung von «Künstlicher Intelligenz» (KI) bei der Bearbeitung von Personendaten auf den Plan. Während private Anbieter und Nutzende von (oft Cloud-basierten) KI-Diensten regelmässig mit überwiegenden eigenen Interessen, der Einwilligung der betroffenen Personen und vertraglichen Ausschlüssen der Verantwortlichkeit operieren können, stellen sich für öffentliche Behörden zahlreiche Fragen insbesondere zur Gesetzmässigkeit, zur Zweckbindung, zur Richtigkeit des Outputs und zur Verantwortung.

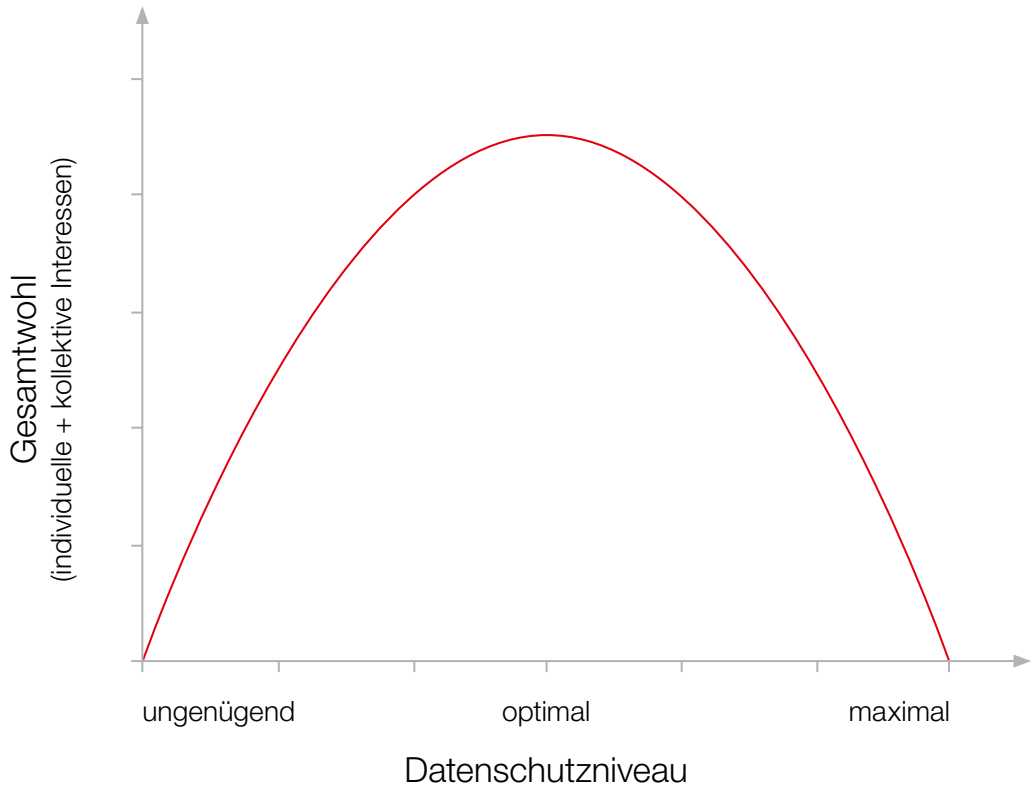
Der vorliegende Bericht vermittelt einen Einblick in die Breite der behördlichen Tätigkeiten, bei welchen sich Datenschutzfragen stellten, mit denen die DSA im Rahmen ihrer Beratungs- und Aufsichtsaufgaben im Berichtsjahr befasst wurde.

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.

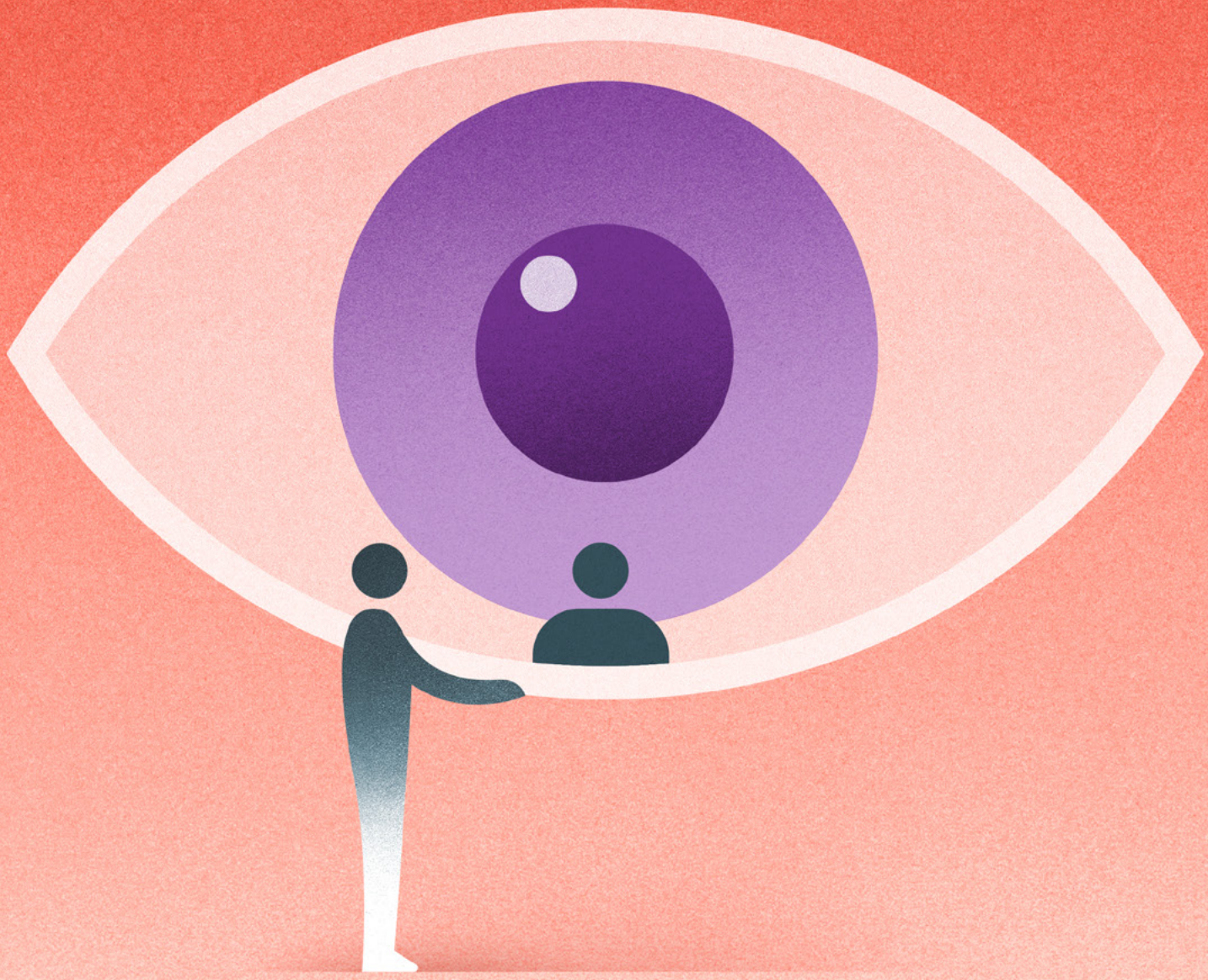
Das Datenschutzgesetz (KDSG) konkretisiert die Pflichten der Behörden beim Bearbeiten von Personendaten, wobei nebst der Verwaltung auch weitere Träger von öffentlichen Aufgaben, z. B. Schulen und Spitäler, als Behörden gelten. Das «Bearbeiten» umfasst jeden Umgang mit Personendaten, wie das Beschaffen, 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 2023 verfügte die DSA über einen Personalbestand von 650 %, 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, Sicherheit), die Staatskanzlei (STA) und 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 sowie der Wirtschafts-, Energie- und Umweltdirektion, bei Videoüberwachungen und bei Fragen von Kirchgemeinden.

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

Stephanie Siegrist (wissenschaftliche Mitarbeiterin Recht) ist Juristin und Historikerin und arbeitete seit 2021 bei der DSA. Sie war in den Bereichen Gesundheit und Bildung tätig und hauptsächlich für Auskunfts- und Beratungsgeschäfte, Vorabkontrollen, Videoüberwachungen und Stellungnahmen zu Erlassen zuständig.

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 Jahr 2023 betrug der Betriebsaufwand der DSA insgesamt TCHF 230. Davon wurden ca. 80 % (TCHF 182) 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, ist die DSA daran, jenes verwaltungsinterne Netzwerk von «Multiplikatoren» intensiver zu pflegen und weiter auszubauen. Im Jahr 2023 führte sie erneut zwei Anlässe mit allen Kontaktstellen für Datenschutz und einen ersten Anlass mit den I-SIVE der Direktionen und der STA durch, um den Austausch mit und auch unter diesen zu verstärken. Zur Überprüfung der Erreichung ihrer strategischen Ziele führte die DSA eine «Zufriedenheitsumfrage» bei ihren wichtigsten Ansprechpersonen innerhalb der Kantonsverwaltung (Generalsekretariate, Gremien für die Digitalisierung, Kontaktstellen für Datenschutz, I-SIVE) sowie bei den Hochschulen und Gesundheitsinstitutionen durch. Der Rücklauf von 69 % mit überwiegend positiven Antworten und weiterführenden konstruktiven Anregungen übertraf die Erwartungen erheblich.

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 (FK) 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

Neues Datenschutzgesetz des Bundes

Am 1. September 2023 trat das totalrevidierte DSG des Bundes in Kraft. Es gilt nur für Bundesbehörden und private (insbes. gewerbliche) Datenbearbeiter, nicht jedoch für kantonale und kommunale Behörden. Für diese gilt grundsätzlich nur das KDSG, das sich zurzeit ebenfalls in Revision befindet (siehe Ziff. 6.2).

Etwas schwieriger wird es, wenn der Kanton oder eine Gemeinde einer privatrechtlichen Organisation eine öffentliche Aufgabe überträgt (durch Gesetz oder einen Leistungsauftrag): Dann wird die Organisation zu einer «Behörde» im Sinne des kantonalen Datenschutzgesetzes und untersteht diesem für alle Datenbearbeitungen, welche sie bei der Erfüllung der übertragenen Aufgabe ausführt. Für die Bearbeitung der Daten des eigenen Personals gilt jedoch – weil dem Privatrecht zugehörig – das DSG.

Noch einmal anders liegen die Dinge dann, wenn eine kantonale oder kommunale Behörde ein privatrechtliches Unternehmen als Hilfsperson für Datenbearbeitungen beizieht, für welche die Behörde weiterhin verantwortlich bleibt (sog. «Auftragsbearbeitung»): Als Private untersteht die Hilfsperson grundsätzlich nur dem DSG. Die Behörde muss ihr aber im Dienstleistungsvertrag sämtliche Pflichten und Verbote (z. B. einer Nutzung der Daten für eigene Zwecke) überbinden, die nötig sind, damit auch das KDSG eingehalten wird. Es darf ja nicht sein, dass die Grundrechte der betroffenen Personen weniger gut geschützt sind, weil sich die verantwortliche Behörde bei der Erfüllung ihrer Aufgaben von Dritten unterstützen lässt. Artikel 28 des neuen Gesetzes über die digitale Verwaltung (DVG) sieht deshalb vor, dass die Behörde sicherstellen muss, dass die Auftragsbearbeiterin die Daten nur so bearbeitet, wie die Behörde selbst es tun dürfte, dass sie die Datensicherheit gewährleistet und Unterbeauftragte nur beizieht, wenn die verantwortliche Behörde vorgängig zugestimmt hat. Als schweizweite Besonderheit sieht der heutige Artikel 16 KDSG vor, dass Beauftragte ebenfalls dem kantonalen Gesetz (und damit sowohl diesem wie dem DSG) unterstehen; die Regelung soll in der laufenden KDSG-Revision im Sinne der vorstehenden Ausführungen (und der neuen Regelung von Art. 28 DVG) geändert werden.

Die Frage des anwendbaren Datenschutzrechts und damit auch der Aufsichtszuständigkeit führte im Berichtsjahr zu zahlreichen Anfragen von kantonalen und kommunalen Behörden sowie zu einem intensiven Austausch zwischen den kantonalen Datenschutzbehörden unter sich und mit dem EDÖB.

Microsoft 365 in der Kantonsverwaltung

Die im vorstehenden Abschnitt geschilderten gesetzlichen Anforderungen für den Beizug von Hilfspersonen gelten auch dann, wenn die Beauftragte ihre Leistungen auf ihrer eigenen – oftmals über verschiedene Standorte verteilten – Infrastruktur in hochstandardisierter Form für eine Vielzahl von unterschiedlichen Kunden erbringt. Bei Cloud-Diensten von international tätigen Anbietern (sog. «Hyperscalern») wie Microsoft hat die verantwortliche Behörde meist kaum Einfluss auf die vertragliche Vereinbarung und kann deren Einhaltung auch nicht wirksam kontrollieren. Selbst wenn die Vereinbarung den datenschutzrechtlichen Anforderungen formell genügt (was beim Beitritt zum Rahmenvertrag 2022–2025 der Schweizerischen Informatikkonferenz mit Microsoft der Fall ist), verliert die Behörde weitgehend die Kontrolle darüber, welche Daten (inkl. solche, die der Anbieter selbst über die Nutzenden der Cloud-Dienste erhebt) wo (geografisch) zu welchen Zwecken bearbeitet werden und wer alles (inkl. Subunternehmen) Einsicht in die Daten nehmen kann. Ist der Anbieter einer ausländischen Rechtsordnung – z. B. dem amerikanischen CLOUD Act – unterworfen, besteht zudem das rechtliche Risiko, dass ausländische Behörden in einer Weise auf die Daten zugreifen, welche gegen das hiesige Recht verstossen würde. Entsprechend verbleiben zahlreiche Risiken für die Grundrechte der betroffenen Personen, die mit geeigneten technischen und organisatorischen Massnahmen teils beseitigt werden können, teils aber auch nicht.

Im Hinblick auf die geplante Einführung von M365 in der Kantonsverwaltung besprachen das KAIO und die DSA in zahlreichen Meetings die einzelnen Risiken und die möglichen Massnahmen zu deren Reduktion oder Beseitigung. Die trotz Massnahmen verbleibenden Restrisiken – insbesondere der Kontrollverlust gegenüber Microsoft und ausländischen Behörden, die fehlende Überprüfbarkeit der vertraglichen Zusagen, rasche Änderungen der Dienste und bei den Subunternehmern sowie die erhöhte Abhängigkeit von Microsoft – wurden vom KAIO in einem Bericht zuhanden des Regierungsrates ausführlich und ehrlich dargestellt. Als Eckpunkte für die Nutzung von M365 wurde festgelegt, dass die Office-Applikationen (Word, Excel, PowerPoint und Outlook) weiterhin lokal installiert sind und die Cloud-Dienste (SharePoint, OneDrive und Teams) nicht für besonders schützenswerte Personendaten oder Daten unter einer besonderen Geheimhaltungspflicht (z. B. von Gesundheitsfachpersonen, im Sozialhilfe- oder im Sozialversicherungsbereich) genutzt werden dürfen.

In ihrer Stellungnahme zum Bericht hielt die DSA fest, dass die verbleibenden Restrisiken nur dann als tragbar erachtet und akzeptiert werden können, wenn sich der Regierungsrat vergewissert, dass die Cloud-Dienste unverzichtbare

Vorteile gegenüber einer lokalen Lösung bringen, welche die neuen Risiken aufzuwiegen vermögen. Für den Betrieb von M365 wies die DSA zudem darauf hin, dass das Modell der geteilten Verantwortung, wonach Microsoft ihre Dienste stets weiterentwickeln und in rascher Folge technisch verändern kann und der Kanton Bern neue Risiken selbst erkennen, bewerten und bewältigen muss, neue Herausforderungen bringt, für die noch keine bewährten Strategien bestehen.

Mit dem Beschluss, wonach er die im Bericht ausgewiesenen Restrisiken anerkennt und akzeptiert, übernahm der Regierungsrat die datenschutzrechtliche und politische Verantwortung für jene Risiken.

Datenschutzlexikon für die Volksschule

Das Amt für Kindergarten, Volksschule und Beratung hatte im zweiten Quartal 2020 ein Projekt zur Überarbeitung des in der Zwischenzeit veralteten Leitfadens «Datenschutz in den Volksschulen des Kantons Bern» aus dem Jahr 2009 gestartet. Die DSA wirkte von Anfang an mit beratender Stimme in dem für alle Beteiligten aufwändigen Projekt mit, welches Ende 2023 seinen erfolgreichen Abschluss fand. Das neue «Datenschutzlexikon für die Volksschule» ist eine digitale Lösung (publiziert unter https://www.lp-sl.bkd.be.ch/de/start/schulleitungen/datenschutzlexikon.html) und richtet sich an Lehrkräfte, Schulleitungen, Schulverwaltungen, Schulbehörden, Fachpersonen und Eltern, die Fragen zu Datenbearbeitungen im Volksschulbereich haben. Im Datenschutzlexikon finden sich derzeit über 70 alphabetisch geordnete Stichwörter zu den wichtigsten Begriffen, Grundsätzen und Informationen zum Datenschutz sowie Antworten zu den in der Praxis am häufigsten gestellten Fragen. Zusätzlich werden drei Merkblätter zu den Cloud-Diensten von Microsoft, Google und Apple angeboten. Das Datenschutzlexikon soll den Volksschulen helfen, Antworten auf die wichtigsten datenschutzrechtlichen Fragestellungen eigenständig zu finden und sich darin zu befähigen.

Publikation von alten Staatskalendern im Internet

Im Zuge einer aufsichtsrechtlichen Anzeige stellte sich die Frage, ob die Universität Bern über eine hinreichende gesetzliche Grundlage für die Veröffentlichung früherer Jahrgänge des bernischen Staatskalenders im Internet verfügt. Die Staatskalender enthalten Angaben über die damaligen Staatsangestellten, folglich Personendaten, und deren Veröffentlichung im Internet führt zu erhöhten Risiken für die betroffenen Personen, weil die Daten weltweit von automatisierten Systemen gesammelt und für beliebige – auch illegale – Zwecke weiterverwendet werden können. Im Verlauf des Austauschs mit der Universität Bern zeigte sich, dass keine Rechtsgrundlage für die Internet-Publikation besteht, weshalb die Universität die Publikation in der Folge einstellte. Vor Ort in der Universitätsbibliothek oder im Staatsarchiv dürfen die früheren Staatskalender weiterhin von jeder Person eingesehen werden.

Enthalten die Staatskalender keine Personendaten mehr, dürfen sie auch ohne gesetzliche Grundlage im Internet publiziert werden. Eine anonymisierte (geschwärzte) Fassung darf deshalb ohne weiteres wieder online publiziert werden. Zudem enden mit dem Tod einer Person auch deren Persönlichkeitsrechte. In Anlehnung an die Archivgesetzgebung darf vermutet werden, dass Personen nach Ablauf des 110. Altersjahrs verstorben sind. Sind Staatskalender genügend alt, enthalten die demnach auch ohne Schwärzung keine schutzwürdigen Personendaten mehr und dürfen im Internet publiziert werden.

Künstliche Intelligenz in der Kantonsverwaltung

Mit dem breiten und kostenlosen Zugang zum Chatbot «ChatGPT» ab Ende 2022 war der Einsatz von KI – hier als Sprachmodell, das auf der Grundlage einer Vielzahl von vorbestehenden Texten darauf trainiert wurde, in der Kommunikation mit Nutzenden Antworten zu geben, die natürlich klingen und inhaltlich relevant sein sollen – plötzlich in aller Leute Munde. Bald stellte sich die Frage, inwieweit die Kantonsverwaltung KI-Systeme datenschutzkonform einsetzen kann. Die allgemein zugängliche Version von ChatGPT nutzt nämlich (wie auch die kostenlose Variante des Übersetzungsdienstes «DeepL») die von den Nutzenden eingegebenen Texte gleichzeitig für ihr eigenes Training, also für einen fremden Zweck, weshalb bei der Nutzung keine Personendaten eingegeben werden dürfen. Zudem werden Daten über die Bedienung des Tools durch die Nutzenden aufgezeichnet und für weitere Produktverbesserungen verwendet. Letztlich kann auch nicht davon ausgegangen werden, dass die Antworten von KI-Systemen inhaltlich richtig sind, weil die Systeme ihre Antworten gar nicht verstehen, sondern bloss mittels statistischer Wahrscheinlichkeiten errechnen.

In Absprache mit der DSA publizierte das KAIO eine Personalinformation, um auf die rechtlichen Schranken und weiteren Risiken bei der Nutzung von KI-Systemen hinzuweisen. Unter der Leitung des Staatsschreibers fand zudem ein Austausch mit Vertreterinnen und Vertreter der Staatskanzlei, der bei dieser angesiedelten Geschäftsstelle Digitale Verwaltung, der Universität Bern und der Berner Fachhochschule, der Stadt Bern sowie der DSA statt.

Datenbekanntgabe mittels offenem Mailverteiler

Ein Bürger machte die DSA darauf aufmerksam, dass ein Amt E-Mails an eine Vielzahl von Empfängern so versandte, dass alle Empfänger für die anderen Empfänger ersichtlich waren. Damit gab das Amt die Namen von natürlichen und juristischen Personen, die in einer Rechtsbeziehung zum Kanton Bern stehen, an Dritte bekannt, ohne dass dies gesetzlich vorgesehen oder zur Aufgabenerfüllung erforderlich war, weshalb die Bekanntgabe als unzulässig anzusehen war. Aufgrund der Möglichkeit, dass sich der Vorgang wiederholen und gegebenenfalls grössere Auswirkungen auf die Rechte der betroffenen Personen haben

könnte, forderte die DSA das Amt auf, geeignete organisatorische Massnahmen zu treffen und aufzuzeigen, damit E-Mails an mehrere Empfänger, die nichts miteinander zu tun haben, nicht mehr offen adressiert werden. Die Massnahmen – der künftige Verzicht auf den Versand von Rundmails mit offenem Verteiler und eine allgemeine Sensibilisierung des Personals für den Datenschutz – erschienen der DSA als angemessen.

Änderung des Polizeigesetzes und neues Gesetz über die Informations- und Cybersicherheit

Im Berichtsjahr wurde der Datenschutzbeauftragte zweimal von einer vorberatenden Kommission des Grossen Rates zur Anhörung über ein Gesetzgebungsgeschäft eingeladen. Die Sicherheitskommission erkundigte sich nach der datenschutzrechtlichen Beurteilung einer Änderung des Polizeigesetzes (PolG), worüber die DSA in ihrem Jahresbericht 2022 ausführlich berichtet hatte (S. 23 f.). Beide dort genannten Probleme waren im Entwurf des Regierungsrates nicht behoben worden: Zwar sollten die Daten aus der automatisierten Fahrzeugfahndung und Verkehrsüberwachung, deren Abgleich mit den polizeilichen Datenbanken keinen Treffer ergaben (sog. «no hits»), nur noch 30 statt 100 Tage aufbewahrt werden, was aber immer noch zu einer unverhältnismässigen Vorratsspeicherung der Daten unbescholtener Bürgerinnen und Bürger führt. Statt eines Verzichts auf die Aufbewahrung erhöhte der Grosse Rat inzwischen die maximale Aufbewahrungsdauer von 30 auf 60 Tage, was aus verfassungsrechtlicher Sicht höchst fragwürdig ist. Die von der DSA weiter kritisierte einseitige Ermächtigung zur Bekanntgabe von Polizeidaten an ausserkantonale Behörden im Abrufverfahren wurde vom Grossen Rat ebenfalls unverändert gutgeheissen.

Die Kommission für Staatspolitik und Aussenbeziehungen befasste sich mit dem Entwurf für ein neues Gesetz über die Informations- und Cybersicherheit (ICSG). Gerade mit Blick auf die zunehmende Bedrohung aus Cyberangriffen sind klare und verbindliche Vorgaben über die Massnahmen zur Gewährleistung der Datensicherheit zentral. Das ICSG soll zeitgemässe Vorschriften primär für Daten bringen, deren Vertraulichkeit, Verfügbarkeit und Integrität aus öffentlichen Interessen zu wahren ist. Die vorgesehenen Grundsätze sind aber genauso für den Schutz von Personendaten zur Wahrung der Grundrechte der betroffenen Personen geeignet. Deshalb soll das revidierte KDSG die Grundsätze des ICSG auch für den Datenschutz als anwendbar erklären.

6.1.2. Betroffene Personen

Auskünfte über Grundeigentümer- und Fahrzeughalterschaft

Mehrere Personen gelangten an die DSA, weil sich sie daran störten, dass Dritte im Internet bzw. mittels SMS-Abfrage erfahren können, wer Eigentümerin oder Eigentümer eines Grundstücks bzw. Halterin oder Halter eines Fahrzeugs ist. In beiden Fällen besteht eine gesetzliche Regelung:

Das Grundbuchrecht des Bundes sieht vor, dass jede Person Auskunft über die Namen und die Identifikation der Eigentümerschaft an einem Grundstück erhält. Und es räumt den Kantonen die Möglichkeit ein, diese Daten elektronisch öffentlich zugänglich zu machen, solange die Daten nur grundstücksbezogen abgerufen werden können und die Auskunftssysteme vor Serienabfragen geschützt sind. Von dieser Möglichkeit hat der Kanton Bern mit dem über das Portal BE-Login zugänglichen Service «GRUDIS public» Gebrauch gemacht. An der allgemeinen Zugänglichkeit von Grundinformationen über die Eigentümerschaft besteht ein öffentliches Interesse: Grundeigentum verschafft ein ausschliessliches Nutzungs- und Verwertungsrecht an einem ursprünglich allgemeinen Gut. Das Grundbuch ist der Ort, wo die Eigentumsverhältnisse öffentlich bekannt gemacht werden, um rechtliche Transparenz zu schaffen: Wenn Dritte ein fremdes Grundstück nicht betreten dürfen, haben sie das Recht zu wissen, wer ihnen die Einschränkung auferlegt.

Das Strassenverkehrsgesetz des Bundes sieht vor, dass die Kantone Name und Adresse der Fahrzeughalterinnen und -halter veröffentlichen können, sofern diese Daten nicht für die öffentliche Bekanntgabe gesperrt sind; diese Sperre kann die betroffene Person voraussetzungslos und gebührenfrei bei der zuständigen kantonalen Behörde eintragen lassen. Das kantonale Strassenverkehrsgesetz verzichtet auf eine Veröffentlichung und sieht stattdessen vor, dass Abfragen im Einzelfall über eine kostenpflichtige Telefonauskunft möglich sind. Jede Person kann die Sperrung der Halterauskunft beim Strassenverkehrs- und Schifffahrtsamt online verlangen.

Fehlzustellung Mailbestätigung über Steuererklärung

Eine ausserkantonal wohnhafte Person erhielt von der Steuerverwaltung ein Mail mit der Eingangsbestätigung für eine Steuerklärung, die sie nie eingereicht hatte, und meldete dies der DSA. Nach Rückfragen der DSA an die Steuerverwaltung stellte sich heraus, dass die Eingangsbestätigung deshalb an einen Namensvetter des Steuerpflichtigen ging, weil dieser bei den Kontaktangaben zur Steuererklärung seine Mailadresse falsch angegeben hatte. Um künftig sicherzustellen, dass die Empfangsbestätigung an die richtige Mailadresse geht, wird die Steuerverwaltung in ihrem System einen zusätzlichen Prüfschritt

einbauen, mit dem sie die in der Steuererklärung angegebenen Mailadressen vorab durch den Versand eines weiteren Mails verifizieren wird.

Erhebung von Daten über die Ehepartner von externen Kursleitenden

Wer als externe Person für den Kanton Bern einen Kurs leitet und dies nicht im Rahmen einer selbständigen Erwerbstätigkeit macht, wird zur korrekten Abrechnung der Sozialversicherungsbeiträge in einem besonderen Modus angestellt. Das Meldeblatt sah vor, dass auch Angaben zur Ehepartnerin oder zum Ehepartner eingetragen werden müssen, darunter die AHV-Nummer, was eine Kursleiterin sehr irritierte. Die Abklärung der DSA beim Personalamt ergab, dass die Angaben dann benötigt werden, wenn eine angestellte Person Beiträge an die Pensionskasse leisten muss, Anspruch auf Familien- und ev. Betreuungszulagen hat oder quellensteuerpflichtig ist. Bei den externen Kursleitenden trifft keiner dieser Fälle zu, weshalb die Ehepartnerangaben nicht erforderlich sind und somit auch nicht erfasst werden dürfen. Die DSA wies zudem darauf hin, dass die AHV-Nummer nach dem AHV-Gesetz des Bundes explizit nur dann systematisch erfasst und weiterbearbeitet werden darf, wenn dafür ein klares fachliches Bedürfnis besteht. Sie empfahl dem Personalamt deshalb, bei den betreffenden Anstellungen auf die Erhebung der Ehepartnerangaben zu verzichten und den Meldeprozess entsprechend anzupassen.

Bekanntgabe der anderen Einsprachen im Baubewilligungsverfahren

Eine betroffene Person erkundigte sich bei der DSA, weshalb die verantwortliche Behörde in einem Baubewilligungsverfahren die Namen und Adressen aller Einspracheparteien den anderen Einsprechenden bekanntgeben dürfe. Die DSA antwortete ihr, dass das Verwaltungsverfahrensrecht den Parteien einen Anspruch auf Akteneinsicht gewähre, soweit nicht überwiegende öffentliche oder private Interesse deren Geheimhaltung erfordern. Als Teil der Verfahrensakten seien die Einsprachen deshalb grundsätzlich allen Parteien offenzulegen. Weil die betreffende Gesetzesnorm (Art. 23 des Gesetzes über die Verwaltungsrechtspflege [VRPG]) im Fall von Mehrparteienverfahren als unklar erscheinen kann, empfahl die DSA im Vernehmlassungsverfahren zur Revision des VRPG eine entsprechende Präzisierung des Wortlauts (siehe auch den Jahresbericht 2022, S. 20 f.).

Einsicht in das Vollzugsverlaufsjournal einer Justizvollzugsanstalt

Ein Eingewiesener wandte sich an die DSA, weil sein Gesuch um Einsicht in die ihn betreffenden Einträge im Vollzugsverlaufsjournal der Justizvollzugsanstalt aus grundsätzlichen Überlegungen abgewiesen wurde. Laut der Anstalt sei das Journal ein Arbeitsinstrument der Mitarbeitenden und nicht für die Eingewiesenen bestimmt; nur die Vollzugsberichte seien Teil der Vollzugsakten und für die

Eingewiesenen einsehbar. Aus Sicht der DSA ist eine generelle Verweigerung der Einsicht nicht haltbar: Das Recht auf Einsicht in die eigenen Daten ist in der Kantonsverfassung als Grundrecht ausdrücklich verankert; es müssen «wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen Dritter» (siehe Art. 21 Abs. 4 KDSG) entgegenstehen, damit die Einsicht verweigert werden darf. Zudem muss eine allfällige Einschränkung verhältnismässig sein und darf nur im Umfang erfolgen, im dem tatsächlich überwiegende Interessen entgegenstehen: Statt einer generellen Verweigerung sind Daten, in die keine Einsicht gewährt werden darf (z. B. zum Schutz des Personals), abzudecken. Ist dies nicht möglich, ist immer noch indirekt Auskunft zu erteilen (Art. 21 Abs. 1 KDSG). In jedem Fall ist eine Einschränkung des Rechts auf Einsicht und Auskunft im Einzelfall so zu begründen, dass der Entscheid für die betroffene Person nachvollziehbar ist. Der blosse Hinweis, dass das Journal nicht für die Eingewiesenen bestimmt ist und sich diese mit den Vollzugsberichten begnügen müssen, reicht als Begründung kaum. Die DSA empfahl der Anstalt, ihren Entscheid in Wiedererwägung zu ziehen, und bot an, an einer datenschutzkonformen und praxistauglichen Klärung der Fragestellung beratend mitzuwirken. Das Amt für Justizvollzug zog es jedoch vor, dass die Sicherheitsdirektion als Aufsichtsbehörde auf die Beschwerde des Eingewiesenen hin über die Angelegenheit entscheidet.

Offen Zustellung von Zahlungsbefehlen durch die Post

Wiederholt melden sich bei der DSA Personen, die sich in ihrer Privatsphäre verletzt fühlen, weil ihnen eine Mitarbeiterin oder ein Mitarbeiter der Post einen betreibungsrechtlichen Zahlungsbefehl offen überreichten und also dessen Inhalt einsehen konnten. Das Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) sieht vor, dass Zahlungsbefehle immer doppelt ausgestellt, einmal für den Schuldner und einmal für den Gläubiger (Art. 70 SchKG). Die Zustellung an den Schuldner geschieht durch das Personal des Betreibungsamtes oder die Post; dabei hat der Überbringer auf beiden Ausfertigungen des Zahlungsbefehls zu bescheinigen, an welchem Tag und an wen die Zustellung erfolgt ist (Art. 72 SchKG). Deshalb kann der Zahlungsbefehl nicht in einem verschlossenen Umschlag übergeben werden. Der Gesetzgeber hat die Nachvollziehbarkeit der für das weitere Verfahren wichtigen Übergabe höher gewichtet als das Geheimhaltungsinteresse der Schuldnerin oder des Schuldners.

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 und für Mitarbeitende der Schuladministration. Seit 2020 findet auch jährlich ein Kurs für Mitarbeitende von Kirchgemeindesekretariaten und seit 2021 eine Ausbildung für Kirchgemeindebehörden zum Thema «Datenschutz in Kirchgemeinden» statt. An den Kursen erläutern die Rednerinnen und Redner 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.

Ebenfalls an das Gemeindepersonal im Bereich der Volksschule richteten sich die Referate von Vertretern der DSA am Netzwerktreffen «Datenschutz und Datensicherheit» des Verbands Schulbehörden Kanton Bern und an der Volksschule Seedorf.

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 (Klausur der Geschäftsleitung der Regierungsstatthalterinnen und Regierungsstatthalter, Weiterbildung der Abteilung Asyl und Flüchtlinge des Amtes für Integration und Soziales, Community-Treffen der Pädagogischen Hochschule Bern im Bereich Medien und Informatik an den Volksschulen, Jurist/innen-Tagung des Verbands der Kantonalen Gebäudeversicherungen) und teils über spezifische Themen. Ein wiederkehrendes Thema war der Datenschutz beim Cloud-Computing (Weiterbildung des Regierungsstatthalteramts Frutigen-Niedersimmental, Gastvortrag im Rahmen der Vorlesung «Datenschutzrecht» der Universität Luzern, Referate an der Cloud Tagung 2023 der Digitalen Verwaltung Schweiz, der Herbsttagung der Vereinigung Gesundheitsinformatik Schweiz, beim Team «Swiss Government Cloud» des Bundesamts für Informatik und Telekommunikation sowie an der Tagung DINAcon 2023). Ausserdem referierte der Datenschutzbeauftragte über den Datenschutz beim Lernen und Arbeiten mit Künstlicher Intelligenz (Schulthess Forum Digitalisierung der Jugend) sowie über die Datenschutzberatung und -aufsicht bei der Digitalisierung (Tagung «Die Zukunft des Datenschutzes in der digitalen Verwaltung» der Universität Basel).

6.2 Formelle Stellungnahmen

Totalrevision des kantonalen Datenschutzgesetzes

Mit einer Totalrevision des kantonalen Datenschutzgesetzes soll dieses modernisiert und an europäische Vorgaben – namentlich die revidierte Datenschutzkonvention des Europarats und die EU-Richtlinie über den Datenschutz im Polizei- und Strafbereich – angepasst werden. Im Berichtsjahr fand die öffentliche Vernehmlassung zum Vorentwurf für das neue KDSG statt, an dessen Vorbereitung die DSA intensiv beteiligt war. Weil der Vorentwurf eine neue Regelung enthielt, die in den Vorarbeiten nicht diskutiert worden und hochproblematisch war, beschränkte sich die DSA in ihrer Stellungnahme auf jene Regelung. Und zwar sollte es den Behörden neu erlaubt sein, Personendaten zur Bearbeitung durch Hilfspersonen auch dann ins Ausland zu übermitteln, wenn dort kein angemessener Datenschutz besteht und dies auch nicht durch geeignete vertragliche Vereinbarungen – welche ausländische Behördenzugriffe nicht auszuschliessen vermögen – kompensiert werden kann. Begründet wurde dies mit dem Interesse der Verwaltung an der Nutzung von amerikanischen Cloud-Diensten, welche im Moment nur eingeschränkt möglich ist, weil die USA mit ihrer Gesetzgebung zur nachrichtendienstlichen Massenüberwachung gegenwärtig nicht als Land mit einem angemessenen Datenschutz gelten. Diese Angemessenheit setzt nicht voraus, dass ein Land das gleiche Datenschutzgesetz hat wie die Schweiz bzw. der Kanton Bern. Verlangt wird «bloss», dass die fundamentalsten Grundsätze der Verfassung – eine hinreichend bestimmte Rechtsgrundlage für Grundrechtseingriffe, die Wahrung der Verhältnismässigkeit und ein minimaler Rechtsschutz für die betroffenen Personen – eingehalten werden. Diese Grundsätze sind so elementar, dass die Datenschutzkonvention des Europarats seit 2001 verlangt, dass Personendaten nur bei einem angemessenen Datenschutz in ausländische Staaten übermittelt werden dürfen. Deshalb würde die beabsichtigte Regelung, sollte sie tatsächlich in das Gesetz aufgenommen werden, gegen die Bundesverfassung und die für den Kanton Bern verbindliche Europaratskonvention verstossen; eine Beschwerde an das Bundesgericht würde zur Aufhebung der Regelung führen. Die DSA hat ihre Stellungnahme mit der ausführlichen Begründung ihrer Einwände auf ihrer Webseite (www.be.ch/dsa > Aktuell) publiziert.

Revision der Informationsverordnung

Das vom Grossen Rat im Jahr 2022 revidierte Informationsgesetz (neu: Informations- und Medienförderungsgesetz [IMG]) ist per 2024 in Kraft getreten. Deshalb wurde im Berichtsjahr auch die zugehörige Ausführungsverordnung, die neu Verordnung über die Information und die Medienförderung (IMV) heisst, totalrevidiert. In Veröffentlichungen der Behörden durften schon bislang Personendaten enthalten sein, soweit nicht überwiegende Interessen – namentlich der

Betroffenen – entgegenstehen. Unter dieser Voraussetzung sieht Artikel 15b IMG neu vor, dass Personendaten auch im Internet bekanntgegeben werden dürfen; sie sind jedoch aus der Publikation zu entfernen, sobald das öffentliche Interesse an ihrer Kenntnisnahme nicht mehr besteht. In der neuen IMV waren dazu zwei Punkte näher zu regeln: Einerseits können bei einer Publikation im Internet besondere Risiken für eine betroffene Person entstehen, etwa dass sie oder Familienangehörige aufgrund der Information im Ausland verfolgt werden oder ihr die Staatsangehörigkeit aberkannt wird. Vor der Publikation im Internet ist deshalb eine zusätzliche Interessenabwägung vorzunehmen; überwiegt das Interesse am Schutz der betroffenen Person, ist auf die Online-Publikation zu verzichten, soweit die Information nicht in anonymisierter (geschwärzter) Form erfolgen kann. Als zweiter Punkt wurde präzisiert, dass die Löschung der Personendaten aus Internet-Publikationen nach schematischen Vorgaben erfolgen und sich nach Publikationskategorien richten kann. Dies erlaubt den Behörden, bereits bei der Publikation Fristen zu hinterlegen, nach deren Ablauf die Publikation bzw. die darin enthaltenen Personendaten automatisch entfernt werden.

Revision des Archivierungsgesetzes

Im Mitberichtsverfahren zur Verabschiedung des Entwurfs für eine Teilrevision des Archivierungsgesetzes (E-ArchG) hatte die DSA keine Bemerkungen mehr anzubringen, weil sie bereits in die Vorarbeiten substanziell einbezogen wurde und die aus Datenschutzsicht relevanten Fragen im Gesetzesentwurf oder im zugehörigen Vortrag geklärt werden konnten. Eine solche Frage ist der Umgang mit Daten, die einer besonderen Geheimhaltungspflicht – etwa dem Berufsgeheimnis von Gesundheitsfachpersonen – unterstehen: Damit diese Unterlagen mit geheimnisgeschützten Daten zur Ablieferung an das Staatsarchiv anbieten können, müssen sie insoweit von ihrer Geheimhaltungspflicht befreit werden (Art. 8 Abs. 3 E-ArchG). Übernimmt das Archiv vorzeitig Unterlagen, für welche die Aufbewahrungsfrist noch läuft, wird es während dieser Zeit zur Hilfsperson der Geheimnisträgerin oder des Geheimnisträgers und damit selbst zur Geheimhaltung verpflichtet; um Dritten den Zugang zu den betreffenden Unterlagen gewähren zu können, müsste es sich von der gleichen Behörde vom Geheimnis entbinden lassen wie die abliefernde Person (Art. 18a Abs. 1 E-ArchG). Auch nach Ablauf der Aufbewahrungsfrist sind besondere Geheimhaltungspflichten – denen Geheimnisträgerinnen und Geheimnisträger regelmässig bis zum eigenen Tod unterstehen – zu berücksichtigen (Art. 17 Abs. 1 und Art. 20 E-ArchG). Zwar untersteht das Archiv dann keiner eigenen Geheimhaltungspflicht mehr, die Unterlagen dürfen bei ihm aber nicht einfacher erhältlich sein als bei der zur Geheimhaltung verpflichteten Person selbst. Mit anderen Worten muss das Archiv bei der Beurteilung eines Zugangsgesuchs z. B. zu Forschungszwecken die gleiche Interessenabwägung vornehmen, wie es die zur Entbindung von der Geheimhaltungspflicht zuständige Behörde tun würde, also dem Geheimnis grundsätzlich ein besonderes Gewicht zumessen.

Programm Neues Fallführungssystem: Ausgabenbewilligung

Mit dem Programm «Neues Fallführungssystem (NFFS)» beabsichtigt die GSI, in den Bereichen der Sozialhilfe, des Kindes- und Erwachsenenschutzes sowie der Arbeitsintegration ein einheitliches IT-System für die Fallführung einzuführen. Das Programm NFFS stellt ein gewichtiges und kostenintensives Projekt der digitalen Transformation im Kanton Bern dar. Im neuen System sollen künftig über 80 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. Entsprechend hat die GSI die DSA bereits sehr frühzeitig beratend miteinbezogen. Auch wenn die DSA im Mitberichtsverfahren zum betreffenden Objektkredit von CHF 52 Millionen keine datenschutzrechtlichen Bemerkungen anzubringen hatte, schätzte sie es sehr, von der GSI so vollständig informiert und konsultiert zu werden.

Vereinbarung über die Harmonisierung der Informatik in der Strafjustiz

Das im Jahr 2016 von der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) geschaffene Programm zur Harmonisierung der Informatik in der Strafjustiz (HIS) dient der besseren interkantonalen Abstimmung und Vernetzung im Bereich der Informatik der Strafbehörden. Im Berichtsjahr konsultierte die KKJPD die Kantone zum Entwurf für eine Verwaltungsvereinbarung zwischen dem Bund und den Kantonen, mit welcher neu die öffentlich-rechtliche Körperschaft «HIS Schweiz» mit Sitz in Bern gegründet werden soll. Der Entwurf sieht vor, dass auf Rechtsfragen beim Betrieb von HIS Schweiz – also für deren Selbstorganisation und -verwaltung – bernisches Recht anwendbar sei soll, namentlich auch das kantonale Datenschutzgesetz. Laut dem erläuternden Bericht wäre deshalb die DSA die zuständige Aufsichtsstelle für die HIS Schweiz. Auf Antrag der DSA stellte der Kanton Bern in seiner Stellungnahme zum Vereinbarungsentwurf Folgendes fest: Das KDSG hält fest, dass die DSA nur der Verfassung und dem Gesetz verpflichtet ist (Art. 33a KDSG). Anders als ein formelles Konkordat ist eine interkantonale Verwaltungsvereinbarung nicht geeignet, um der DSA neue Aufgaben zuzuweisen. Der DSA ist es aber erlaubt, gestützt auf eine von ihr selbst abgeschlossene Vereinbarung Aufgaben der Datenschutzaufsicht in anderen öffentlich-rechtlichen Körperschaften zu übernehmen (Art. 36a Abs. 4 KDSG). Die betreffenden Leistungen sind angemessen zu entschädigen, da sonst die finanzielle Unabhängigkeit der DSA beeinträchtigt würde. In diesem Sinne haben etwa die mit den Gesamtschweizerischen Geldspielkonkordat geschaffenen Organisationen die DSA als Aufsichtsstelle bezeichnet und mit ihr eine Vereinbarung inklusive Entschädigungsregelung abgeschlossen.

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 133 Vorabkontrollen und Vorprüfungen (Vorjahr: 134) zu Informatikprojekten bearbeitet und dabei 63 (94) Geschäfte abgeschlossen. Die im Vergleich zum Vorjahr tiefere Zahl der Abschlüsse liegt am sehr grossen Umfang und der hohen Komplexität mehrerer Geschäfte wie dem SAP-Projekt mit mehreren Etappen, der Einführung von M365 in der Kantonsverwaltung (welche über 10 neue oder geänderte ISDS-Konzepte umfasst) und der Digitalisierungsprojekte der Insel Gruppe.

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.

Einführung von M365 bei verschiedenen Behörden

Wie unter Ziff. 6.1.1. oben ausgeführt, bringt die Auslagerung von Datenbearbeitungen in Cloud-Dienste wegen des damit verbundenen Kontrollverlusts der verantwortlichen Behörde eine Reihe von zusätzlichen 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. Jede Behörde, welche eine Einführung von M365 in Betracht zieht, kommt daher nicht umhin, ihre konkreten fachlichen Bedürfnisse zu definieren, die von ihr bearbeiteten Daten und deren Schutzbedarf zu beschreiben, die Risiken für alle betroffenen Personen vollständig zu benennen und geeignete Massnahmen zu treffen, um jene Risiken zu senken oder auf ein tragbares Mass zu reduzieren – was auch die Evaluation von alternativen Produkten und bei hohen Restrisiken den (teilweisen) Verzicht auf die Nutzung einzelner Cloud-Dienste umfasst. Für die verbleibenden Risiken, die als tragbar erachtet werden, muss das oberste Leitungsorgan der Behörde die datenschutzrechtliche Verantwortung übernehmen. Jede Behörde, welche eine Einführung von M365 plant, muss sich deshalb bewusst sein, dass sie sich auf ein anspruchsvolles und zeitaufwändiges Vorhaben einlässt.

Entsprechend konnten die parallel zur Vorbereitung des Risikoberichts des KAIO an den Regierungsrat (siehe Ziff. 6.1.1. oben) angelaufenen Vorabkontrollen der zahlreichen ISDS-Konzepte zur Einführung von M365 in der *Kantonsverwaltung* im Berichtsjahr noch nicht abgeschlossen werden. Die DSA unterzog alle Konzepte einer ersten Prüfung und stellte die Entwürfe ihrer Vorabkontrollberichte mit einer Reihe von Feststellungen und Empfehlungen dem KAIO zur Stellungnahme und Überarbeitung bzw. Ergänzung der ISDS-Unterlagen zu. Ein wesentlicher noch offener Punkt sind die organisatorischen, prozessualen und technischen Massnahmen zur Gewährleistung der Informationssicherheit und des Datenschutzes beim Betrieb eines Verbunds von Diensten, welche sich technisch permanent verändern und deshalb laufend auf neue Risiken hin geprüft und beurteilt werden müssen.

Ein Abschluss der Vorabkontrolle – welche sich über vier «Iterationen» (Berichtsentwürfe der DSA mit Befunden und Stellungnahmen der Behörde) erstreckte – war im Fall der *Universität Bern* möglich, welche M365 bis Ende 2024 einführen will. Wie in der Kantonsverwaltung dürfen die Nutzenden auch hier keine besonders schützenswerten oder einer gesetzlichen Geheimhaltungspflicht unterstehenden Personendaten in Cloud-Diensten bearbeiten. Nichts desto trotz waren die Anwendungsfälle, die dabei bearbeiteten Daten, die Erforderlichkeit der teilweisen Auslagerung, die Einbindung in die lokale IT-Infrastruktur, die Massnahmen zur Risikosenkung und die Übernahme der Restrisiken durch die Universitätsleitung sauber zu dokumentieren und zu prüfen.

Auch die *Insel Gruppe AG* beabsichtigt die Einführung von M365 bis Ende 2024. Dabei geht es primär um die Büroautomatisation, in gewissen Fällen sollen aber auch besonders schützenswerte Angaben über die Gesundheit von Patienten bearbeitet werden können. Entsprechend liegt der Fokus der laufenden Vorabkontrolle bei den technischen und organisatorischen Massnahmen zum

Schutz der Vertraulichkeit der betreffenden Daten, welche erhöhte Anforderungen erfüllen müssen.

Nutzung der AWS-Cloud für die Bearbeitung von medizinischem Bildmaterial

Das Institut für Gewebemedizin und Pathologie plante die Digitalisierung des Bildmaterials von pathologischen Proben und des zugehörigen Befundprozesses einschliesslich der Entscheidungsunterstützung durch KI-Systeme. Wegen des grossen Bedarfs an Speicher- und Rechenkapazitäten sollte das betreffende *Image Management System* mittels Diensten der Amazon Web Services (AWS) betrieben werden. Im Rahmen der Vorabkontrolle zeigte sich, dass das Bildmaterial zuerst pseudonymisiert und erst danach in den Cloud-Diensten bearbeitet wird, so dass die Daten von Dritten keiner bestimmten oder bestimmbaren Person zugeordnet werden können und für diese letztlich gar keine Personendaten darstellen. Damit konnte die Vorabkontrolle abgeschlossen werden, ohne dass besondere Massnahmen zum erhöhten Schutz von Gesundheitsdaten aufgezeigt werden mussten.

Übermittlung von (potenziellen) Personendaten in die USA

Eine neue Smartphone-App des Amts für Landwirtschaft und Natur (LANAT) sollte es interessierten Personen ermöglichen, beim Betreten eines Naturschutzgebiets auf die bestehenden Verbote hingewiesen zu werden und sich auch unabhängig davon Informationen über die Naturschutzgebiete zu erhalten. Dabei wird aus technischen Gründen die *Internet Protocol* (IP-) Adresse des Smartphones an den Anbieter in die USA übermittelt. IP-Adressen gelten dann als Personendaten, wenn sie vom Empfänger – sei es der beabsichtigte oder ein unbefugter Dritter – einer bestimmten oder bestimmbaren Person zugeordnet werden können. Die DSA empfahl dem LANAT, die IP-Adressen wie Personendaten zu behandeln und dafür zu sorgen, dass ihre Übermittlung in die USA rechtmässig erfolgt. Wegen ihrer Gesetzgebung zur nachrichtendienstlichen Massenüberwachung gelten die USA gegenwärtig nicht als Land mit einem angemessenen Datenschutz, so dass Personendaten grundsätzlich nicht dorthin übermittelt werden dürfen (Art. 14a Abs. 1 KDSG). Die Übermittlung ist allerdings erlaubt, wenn die betroffene Person vorgängig darüber informiert wurde und eingewilligt hat. Das LANAT sah daher vor, dass beim erstmaligen Öffnen der App eine Information erscheint und die betroffene Person ihr Einverständnis geben muss, um die App nutzen zu können.

Plattform E-Mitwirkung

Öffentliche Konsultationen, namentlich für Vernehmlassungen zu Erlassentwürfen, wollte der Kanton Bern neu über die elektronische Plattform E-Mitwirkung abwickeln. Die Plattform wird von einem Schweizer Anbieter als *Software-as-a-Service* zur Verfügung gestellt. Dank der konstruktiven Haltung der federführenden STA und der Bereitschaft des Anbieters zu technischen Anpassungen an der Plattform selbst konnten im Laufe der Vorabkontrolle alle Empfehlungen der DSA umgesetzt werden: Diese bemängelte namentlich, dass für Kantonsmitarbeitende anfänglich einsehbar war, welche Personen an der Erarbeitung von Stellungnahmen mitwirkten, die unter Einsatz der Kollaborationsfunktion von E-Mitwirkung erarbeitet wurden; politische Ansichten und Betätigungen gelten als besonders schützenswerte Angaben und gehen – jedenfalls soweit sie bei Einreichung der Stellungnahme nicht offengelegt werden – die Behörden nichts an. Das Problem konnte behoben werden, indem der Anbieter die Angaben, welche er selbst für die Berechtigung der beteiligten Personen auf der Plattform benötigte, für die Behörden nicht mehr sichtbar zu machen. Für den Mail-Versand von Statusmeldungen wie die erfolgreiche Registrierung auf der Plattform oder die Empfangsbestätigung für Stellungnahmen wurde anfänglich ein in den USA ansässiger Dienstleister eingesetzt, der dann aber durch einen europäischen Anbieter ersetzt werden konnte. Schliesslich empfahl die DSA der STA zahlreiche Anpassungen an den Nutzungs- und Datenschutzbestimmungen, welche vollständig umgesetzt wurden.

Digitalisierung des Postverkehrs mit der Kantonsverwaltung

Im Berichtsjahr unternahm die Kantonsverwaltung weitere Schritte bei der Digitalisierung des Postverkehrs, was zu entsprechenden Vorabkontrollen führte. Mit dem Projekt «Digipost@BE» wurde bei verschiedenen Ämter die digitale Verarbeitung der eingehenden Briefpost eingeführt: Die Post wird an einem zentralen Ort geöffnet, gescannt und der zuständigen Behörde digital zur weiteren Bearbeitung zugestellt. Dabei war sicherzustellen, dass als geheim, persönlich, vertraulich oder privat gekennzeichnete Briefpost ungeöffnet bleibt und den adressierten Stellen weiterhin separat per Briefpost zugestellt wird. Zudem kommt ein KI-gestütztes Lernmodul zum Einsatz, welches daraufhin trainiert werden kann, die eingehenden Dokumente effizienter zuordnen zu können, etwa durch das Erlernen der Koordinaten von bestimmten Inhaltsfeldern. Bei der Konfiguration des Lernmoduls definiert die jeweils empfangende Behörde, welche Daten für das Training verwendet werden dürfen; sie muss dafür sorgen, dass sich dabei nicht um Personendaten handelt.

Auch der umgekehrte Weg, die Zustellung von Dokumenten der Verwaltung an die Bürgerinnen und Bürger, soll digital erfolgen können. Unter Beizug der Post stellt der Kanton Bern mit «BE-ePost» einen digitalen Briefkasten zur freiwilligen Benutzung zur Verfügung. In der Vorabkontrolle prüfte die DSA namentlich das Vorhandensein der notwendigen Rechtsgrundlagen, die Wahrung

der Vertraulichkeit und die sichere Übermittlung der Daten sowie die Möglichkeit, jederzeit zur postalischen Zustellung der Dokumente zurückkehren zu können. Als erster Anwendungsfall können interessierte Personen über ihr BE-Login-Konto und die ePost-App die Steuerratenrechnungen auf diesem Weg erhalten.

Digitale Transformation der Insel Gruppe AG

Die Insel Gruppe AG beabsichtigt, eine Vielzahl von Informatiksystemen durch das neue Klinikinformationssystem (System für die Dokumentation der Behandlung und Steuerungssystem für die Bettenbelegung, Einsatzplanung, Zimmerreinigung usw.) des amerikanischen Anbieters EPIC abzulösen. Dabei soll von einem am medizinischen Fall orientierten zu einem patientenzentrierten Ansatz übergegangen werden, der die interdisziplinäre und interprofessionelle Behandlung erleichtert. Damit alle Standorte, Kliniken, Medizinbereiche und Berufsgruppen bei Bedarf zusammenarbeiten können, sollen die Behandlungsdokumentationen der Patientinnen und Patienten ganzheitlich in einer Akte zentral geführt und nicht mehr fall- bzw. klinikbezogen dokumentiert werden; auf die Daten sollen weitgehende Zugriffsrechte des medizinischen Personals bestehen. Wegen des grossen Umfangs und der hohen Komplexität des Vorhabens sowie des neuen Konzepts für die Aufbewahrung und den Zugang zu den Daten bat die DSA um ihren frühen beratenden Einbezug in das Projekt. Dies ermöglichte bereits vor der Vorabkontrolle einen Austausch über anstehende Meilensteine und datenschutzrechtliche Eckpunkte sowie eine ausführliche Demonstration des Systems vor Ort. Mit Blick auf die Zugriffsberechtigungen wies die DSA von Anfang an darauf hin, dass geeignete Massnahmen zur Gewährleistung des Verhältnismässigkeitsprinzips getroffen werden müssen. Im Rahmen der Vorabkontrolle fanden im Berichtsjahr zwei «Iterationen» statt, wobei sich die Zahl der zunächst 86 offenen Befunde auf 25 reduzierte.

Eng verknüpft mit dem Klinikinformationssystem EPIC ist die ebenfalls zur Vorabkontrolle unterbreitete Fachapplikation «Medical Content Plattform», die das neue *Health Content Management System* der Insel Gruppe AG werden soll. Das in EPIC integrierte System stellt den Fachpersonen einen Grossteil der medizinischen Inhalte in Form von Bildern, Dokumenten, Biosignalen sowie Video- und Audiodateien zur Verfügung, welche in Expertensystemen produziert oder von externen Zuweisenden bzw. Partnerinstitutionen zur Verfügung gestellt werden. Im Berichtsjahr erstattete die DSA ihre dritte und vierte Rückmeldung zur umfangreichen (jeweils wieder überarbeiteten) ISDS-Dokumentation, die Prüfung der erneuten Überarbeitung ist noch im Gang.

Video- und Audioaufzeichnungen bei der Arbeitsvermittlung

Die kantonale Arbeitsmarktverordnung sieht seit 2022 vor, dass das Amt für Arbeitslosenversicherung (AVA) zur Qualitätssicherung und zur Weiterbildung von

Mitarbeitenden Video- und Audioaufzeichnungen von Gesprächen mit Kundinnen und Kunden erstellen kann, sofern alle Beteiligten ausdrücklich einwilligen. Im Berichtsjahr reichte das AVA die betreffenden ISDS-Unterlagen zur Vorabkontrolle ein. In dieser prüfte die DSA namentlich die Umsetzung der Vorgaben zur (freiwilligen!) Einwilligung, die Plattform für die Speicherung der Aufzeichnungen während der Aufbewahrungsfrist und die anschliessende Vernichtung der Daten. Weil für die Qualitätssicherung auch Forschung betrieben werden soll, prüfte die DSA zudem die Bedingungen für eine zulässige Weitergabe der Daten zu Forschungszwecken und das dabei zu beachtende Vorgehen.

Weiterentwicklung «VacMe» für Affenpocken- und andere Impfungen

Die GSI entwickelte die während der Pandemie eingeführte Digitale Lösung COVID-19-Impfung («VacMe») so weiter, dass künftig weitere Impfbedürfnisse wie die Affenpocken-, Influenza- oder Zeckenimpfung damit abgewickelt werden können. Ein wesentlicher Befund in der Vorabkontrolle war der Umstand, dass nicht nur die öffentlichen Leistungserbringer im Bereich der Gesundheitsversorgung, sondern auch die Behörden der Kantonsverwaltung die Daten der impfwilligen bzw. geimpften Personen hätten einsehen und weiterbearbeiten können, wofür keine hinreichende Rechtsgrundlage besteht. Die GSI nahm deshalb technische Anpassungen vor und änderte das Rollen- und Berechtigungskonzept so, dass die Verwaltungsbehörden keinen Zugang zu den Daten mehr hatten. Damit konnte die Vorabkontrolle mit einem positiven Ergebnis abgeschlossen werden.

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 Rücksprache-verfahren zu konsultieren, wobei die KAPO das Ergebnis der Vorabkontrolle der zuständigen Datenschutzaufsichtsstelle – für kantonale Behörden die DSA – berücksichtigt. Betreffend die Anforderungen an die Informationssicherheit und den Datenschutz erarbeitete die DSA eine ISDS-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).

Überwachung der Militärkaserne

Installationen zur Videoüberwachung – namentlich die Standorte der Kameras und die damit aufgenommenen örtlichen Bereiche – sowie das Bedürfnis nach einer solchen Überwachung sind für die DSA sehr viel einfacher verständlich, wenn die konkreten Verhältnisse zusammen mit der verantwortlichen Behörde vor Ort besichtigt werden. Nach einer entsprechenden Besichtigung der Militärkaserne Bern erhielt die DSA die ISDS-Unterlagen für eine Erneuerung der Videoüberwachung zur Vorabkontrolle unterbreitet. Acht Kameras waren im Rahmen der Zutrittskontrolle zur Echtzeitüberwachung vorgesehen, weitere 18 Kameras sollten an verschiedenen Orten zum Schutz des Gebäudes und der auf dem Areal abgestellten (teils militärischen) Fahrzeuge Bildaufzeichnungen machen. Die Prüfung, der grundsätzlich jede Kamera einzeln unterzogen wird, ergab einen zweckkonformen und verhältnismässigen Einsatz der Videoüberwachung.

Neues Anna-Seiler-Haus der Insel Gruppe AG

Für das neue Bettenhochhaus der Insel Gruppe AG war eine umfangreiche Videoüberwachung vorgesehen. Diese bestand aus 75 Kameras, die sich auf das PolG stützen, dem Schutz des Gebäudes sowie des Personals und den Patientinnen und Patienten vor Straftaten dienen sollen und dazu Bilder aufzeichnen. Weitere 63 Kameras dienen nicht polizeilichen Zwecken, sondern der Aufgabenerfüllung im Bereich der Spitalversorgung; dabei handelt es sich um Echtzeitüberwachungen von ausgewählten Orten zum Schutz der Gesundheit der Patientinnen und Patienten. Nach der Beurteilung der DSA wurden sämtliche Kameras für den jeweiligen Zweck in verhältnismässiger Weise eingesetzt und das Bildmaterial für eine angemessene Dauer aufbewahrt. Auf eine Empfehlung betreffend den technischen Schutz der Bilder vor Zugriffen unbefugter Dritter wird die DSA bei der Prüfung der gesamten Videoinfrastruktur zurückkommen.

6.4 Audits

Die DSA hat den gesetzlichen Auftrag, die Anwendung der Vorschriften über den Datenschutz und die Informationssicherheit zu überwachen. Während eine Vorabkontrolle nur den *Soll-Zustand* im Sinne eines Plans, wie eine neue Datenbearbeitung beabsichtigt ist, auf seine rechtliche Konformität und Sicherheit hin beurteilt, wird bei ISDS-Audits die tatsächliche Umsetzung des Plans als *Ist-Zustand* geprüft. Die Audits stellen deshalb in der Aufsichtstätigkeit der DSA eine wichtige Ergänzung zu den Vorabkontrollen dar.

Im Berichtsjahr führte die DSA neun ISDS-Audits durch, wovon eines zusammen mit der FK; die sehr gute Zusammenarbeit zwischen DSA und FK soll auch in Zukunft weitergeführt werden. Ein geplantes Audit konnte aufgrund der schwierigen Ausgangslage bei der geprüften Stelle nicht vollzogen werden. Im Rahmen ihrer risikoorientierten Strategie konzentrierte sich die DSA auf Dienste der ICT-Grundversorgung, wesentliche Fachapplikationen und den Gesundheitsbereich (Spitäler), wo primär der ICT-Grundschutz und die Medizintechnik-Geräte geprüft wurden. Zudem überwachte die DSA die Fortschritte bei der Umsetzung von Empfehlungen aus den in den Vorjahren durchgeführten Audits. Die enge Begleitung der Verbesserungsmassnahmen stellt eine zielführende und wirksame Standardaufgabe der DSA dar.

Allgemeine Erkenntnisse

Die Nachprüfungen zeigten der DSA transparent auf, ob die festgestellten Mängel von den verantwortlichen Behörden wirksam und nachweisbar behoben wurden. Neben erkennbaren Fortschritten musste auch wiederholt festgestellt werden, dass erforderliche Massnahmen teils nicht mit der gebotenen Sorgfalt angegangen wurden. Fehlende Aufmerksamkeit und eine entsprechend verzögerte Umsetzung von ISDS-Massnahmen erhöhen das Risiko, dass auf die sich stets verändernde Bedrohungslage aus kriminellen Cyberaktivitäten nicht rechtzeitig und adäquat reagiert werden kann. Das systematische Erkennen und zeitnahe Adressieren von ISDS-Risiken muss deshalb noch an Aufmerksamkeit gewinnen. Dies gilt auch für die verlangte periodische Überprüfung der Risiken und Massnahmen (Art. 4 Abs. 3 der Datenschutzverordnung [DSV]) zum generellen Erhalt der ICT-Widerstandsfähigkeit.

Bei den Spitälern zeigte sich, dass die Verwaltung der Medizintechnik-Geräte massgeblich von den Lieferanten beeinflusst wird. Aufgrund deren Marktmacht haben die Spitäler teils wenig Einfluss auf die Medizininfrastruktur und deren Betriebssicherheit. Zusätzliche Wartungen zum Erhalt bzw. zur Erhöhung der Sicherheit sind oft mit hohen Kostenfolgen verbunden.

Allgemein überlassen die verantwortlichen Behörden wesentliche Teile ihrer ISDS-Verantwortung den involvierten Dienstleistern und Lieferanten, welche sich nicht im direkten Einfluss- und Kontrollbereich der Behörden befinden. Die Steuerung und Überwachung der Dienstleister und Lieferanten muss noch besser und vor allem auch nachweisbarer wahrgenommen werden.

Fachanwendung socialweb

Mehrere kantonale Schulheime nutzen die Fachanwendung «socialweb» für die Institutionsverwaltung und die Klientenbetreuung. Socialweb ist eine modular aufgebaute webbasierte Softwarelösung für die soziale und sozialpädagogische

Arbeit. Die Prüfung der DSA fand stellvertretend im Pädagogischen Zentrum für Hören und Sprache in Münchenbuchsee statt. Sie umfasste die Bereiche ISDS-Governance (Steuerung der ISDS-Aufgaben), ISDS-Konzepte und Schutzmassnahmen, Prozesse des Benutzermanagements, Outsourcing, Datenhaltung und Schnittstellen, Betriebskontinuitätsmanagement, ICT-Service Continuity Management sowie das Notfall-Krisenmanagement.

Als Ergebnis wurden über alle Prüfbereiche hinweg Befunde festgehalten, welche überwiegend mit einem mittleren ISDS-Risiko eingestuft wurden. Die Revisionsfähigkeit der Fachanwendung war aufgrund der veralteten Dokumentation und damit des unklaren ISDS-Soll-Zustandes eingeschränkt. Ein vollständiges und qualifiziertes Prüfergebnis war daher nicht möglich. Die DSA wird die Umsetzung von Verbesserungsmassnahmen aktiv begleiten.

BE-NET WLAN

Im 2019 hatte die DSA geprüft, inwieweit das vom KAIO im Rahmen der ICT-Grundversorgung BE-NET angebotene drahtlose Netzwerk (Wireless Local Area Network; WLAN) die ISDS-Anforderungen erfüllt. Dabei waren Befunde mit mittleren und tiefen ISDS-Risiken festgehalten worden. In einer Nachrevision wurde nun geprüft, ob die empfohlenen Verbesserungsmassnahmen vollständig und nachvollziehbar umgesetzt und auf ihre Wirksamkeit überprüft wurden.

Die Prüfung ergab, dass nur sechs der 14 Befunde vollständig erledigt waren. Sechs Befunde waren nur teilweise erledigt; zwar wurde mit der Umsetzung begonnen, jedoch bestand noch Anpassungsbedarf. Zwei Befunde waren noch gänzlich offen, so dass die betreffenden Risiken weiterhin bestanden. Immerhin lag eine Planung vor, wonach die Massnahmen zu den Empfehlungen bis Ende Juli 2024 umgesetzt werden sollen. Angesichts der seit der ersten Prüfung verstrichenen Zeit war jenes Ergebnis nicht zufriedenstellend. Die Aufmerksamkeit für eine zeitnahe Umsetzung von Verbesserungsmassnahmen muss weiter erhöht werden. Die DSA wird die Umsetzung der pendenten Massnahmen begleiten.

Rechenzentrum der KAPO

Die FK und die DSA führten eine gemeinsame Prüfung über den Betrieb des Rechenzentrums (RZ) der KAPO durch. Deren Informatik- und Kommunikationsanwendungen werden mehrheitlich in Eigenleistung in eigenen Räumlichkeiten an zwei Standorten in Bern betrieben. Geprüft wurden namentlich das Vorhandensein eines angemessenen ISDS-Kontrollrahmenwerks mit einer nachvollziehbaren Steuerung des RZ-Betriebs, die der Kritikalität der betriebenen Anwendungen angemessene physische Sicherheit sowie die Massnahmen zur Gewährleistung der Netzwerksicherheit. Weiter wurde die Einsatzbereitschaft bei Notfällen und Krisenvorsorge geprüft.

Die Prüfung ergab, dass die für das RZ benutzen Räumlichkeiten historisch gewachsen und gebäudetechnisch nicht für den Betrieb von ICT-Infrastruktur konzipiert wurden. Das Gesamtergebnis der Prüfung liess daher den Schluss zu, dass das aktuelle RZ – auch in Anbetracht der betriebenen kritischen ICT-Anwendungen – nicht den hohen ISDS-Anforderungen und gängigen RZ-Standards sowie guter Praxis entspricht und deshalb mit hohen ISDS-Risiken verbunden ist. Im Zuge des Neubaus des Polizeizentrums Bern soll das RZ der KAPO neu konzipiert werden.

Fachanwendung GERES

Das Gemeinderegistersystem (GERES) dient der Erfüllung der kantonalen Aufgaben im Rahmen der Bundes- und der kantonalen Gesetzgebung im Bereich der Registerharmonisierung, des Ausländerrechts sowie des Rechts über Niederlassung und Aufenthalt der Schweizerinnen und Schweizer. Zudem dient GERES als zentrale Quelldatensammlung für die Erfüllung zahlreicher öffentlicher Aufgaben sowie statistischen Zwecken. Die enthaltenen Daten werden von den Gemeinden geliefert und auf kantonaler Ebene konsolidiert. Der Betrieb von GERES liegt in der Verantwortung des KAIO. Die Prüfung der DSA umfasste die Informationssicherheit, das Change-Management und die Berechtigungsverwaltung sowie das Outsourcing. Weiter wurde geprüft, ob Kontrollen vorhanden sind, welche die Einhaltung der regulatorischen Vorgaben bei der Personendatenbearbeitung sicherstellen.

Das Ergebnis der Prüfung zeigte erfreulicherweise auf, dass nur in zwei von fünf Prüfbereichen Befunde mit mittlerer oder tiefer Wesentlichkeit festgestellt werden mussten. Die Befunde betrafen die Kontrollen, welche sicherstellen, dass die Benutzer keine Zugriffsrechte erhalten, welche sie zur Erfüllung der ihnen zugewiesenen Aufgaben nicht benötigen, und Verzögerungen bei der Datenlöschung. Die DSA wird die Umsetzung der notwendigen Verbesserungsmassnahmen begleiten.

Spitalzentrum Biel: ICT-Grundschutz

Das Spitalzentrum Biel (SZB) ist das öffentliche Zentrumsspital für die Region Biel, Seeland und Berner Jura. Als Akutspital bietet das SZB die gesamte Palette der erweiterten medizinischen Grundversorgung an. In vier interdisziplinären Schwerpunktgebieten ist das Angebot des Zentrumsspitals auch überregional für die medizinische Versorgung der Bevölkerung von Bedeutung. Das SZB weist die Rechtsform einer Aktiengesellschaft auf, welche zu 99 % im Besitz des Kantons Bern ist. Die geprüften Bereiche im SZB fokussierten sich auf die ISDS-Anforderungen im Bereich des ICT-Grundschutzes. Dieser umfasst die alle Massnahmen (Organisation, Verfahren, Hilfsmittel, Infrastruktur und technische Systeme, Daten und Vorkehrungen etc.), welche die

datenschutzkonforme und sichere Abwicklung der Geschäftsprozesse, einschliesslich der Personendatenbearbeitungen, beim SZB unterstützen.

Die Prüfung ergab über nahezu alle Prüfbereiche hinweg Befunde, die teilweise ein mittleres und auch erhöhtes Risiko für den Datenschutz und die Informationssicherheit darstellen. Insbesondere waren im Zeitpunkt der Prüfungshandlungen wesentliche Verfahren und Kontrollen, um Personendaten wie auch ICT-Systeme entsprechend ihrer Klassifizierung und Kritikalität zu sichern und rechtskonform zu betreiben, noch in Arbeit. Dies erhöht das Risiko, dass regulatorische Vorgaben nicht nachvollziehbar eingehalten und die ICT-Systeme nicht den notwendigen Schutz gewährleisten. Die DSA wird die Umsetzung von Verbesserungsmassnahmen begleiten.

Spital SRO AG: ICT-Infrastruktur Medizintechnik

Das Spital Region Oberaargau (SRO AG) ist das regionale Spitalzentrum im Oberaargau. Das Spital Langenthal und seine zwei Gesundheitszentren in Huttwil und Niederbipp sowie der Panorama Park in Herzogenbuchsee bieten eine umfassende medizinische Versorgung für die Bevölkerung der Region. Der Betrieb der ICT-Infrastruktur wird grösstenteils mit internen Ressourcen sichergestellt. Im Rahmen von Projekten und für Dienstleistungen werden auch externe Spezialisten hinzugezogen. Im 2019 hatte die DSA den ICT-Grundschutz bei der SRO AG geprüft. Auf dieser Grundlage stand im Berichtsjahr die Verwaltung der ICT-Medizintechnik im primären Fokus der Prüfung. Die Prüfbereiche umfassten ausgewählte Kontrollen beim Risiko Management, ICT-Betrieb und beim Outsourcing sowie die Rolle des Chief Information Security Officer. Beim ICT-Grundschutz wurde im Sinne einer Nachrevision die Umsetzung der Verbesserungsmassnahmen geprüft.

Die Prüfung bei der Medizintechnik ergab in allen Prüfbereichen Befunde mit teilweise hohem ISDS-Risiko. Dazu gehörte, dass der organisatorische Verwaltungsprozess und die Lebensbetrachtung bei der Medizintechnik noch nicht optimal abgebildet und abgestimmt waren. Vorgaben und Handlungsanweisungen bestanden nur teilweise. Weiter zeigte eine Schwachstellenprüfung eine hohe Anzahl an offenen und bekannten Sicherheitslücken unterschiedlicher Kritikalität bei den am Netzwerk angeschlossenen medizinischen Geräten. Die Ursache dafür liegt auch darin, dass die internen ICT-Verantwortlichen keine Möglichkeit hatten, um veraltete Software der Medizingeräte zu aktualisieren. Dieser Vorgang muss regelmässig durch den Hersteller bzw. Lieferanten autorisiert werden oder erfolgen, was teils nicht systematisch geschieht, sondern nur auf Aufforderung der SRO AG. Ausserdem fallen dafür oftmals sehr hohe Kosten an. Hier besteht ein erkennbares Sicherheitsdefizit, auf das die SRO AG nur teilweise einen direkten Einfluss hat. Dennoch muss die SRO AG die ISDS-Risiken vollumfänglich tragen. Die Hersteller bzw. Lieferanten der Medizintechnik müssen hier ihren Beitrag leisten, damit die ISDS-Verantwortung wahrgenommen werden kann. Die DSA wird die Umsetzung der Verbesserungsmassnahmen begleiten.

Spital STS AG: ICT-Infrastruktur Medizintechnik

Die Spital Simmental-Thun-Saanenland (STS) AG gewährleistet in den Spitälern Thun und Zweisimmen die medizinische Versorgung im westlichen Berner Oberland. Als grösstes öffentliches regionales Spitalzentrum im Kanton Bern stellt die STS AG ein breites Angebot in der Grundversorgung sowie in der spezialisierten Medizin zur Verfügung. Der Betrieb der ICT-Infrastruktur wird grösstenteils mit internen Ressourcen sichergestellt. Für dezidierte Dienstleistungen werden auch externe Spezialisten hinzugezogen. Im 2020 hatte die DSA den ICT-Grundschutz bei der STS AG geprüft. Im Berichtsjahr erfolgte eine Prüfung mit dem gleichen Fokus und den gleichen Prüfbereichen wie bei der SRO AG, wobei allerdings nicht alle Prüfbereiche gleichermassen geprüft werden konnten.

Die Prüfung bei der Medizintechnik ergab in den geprüften Bereichen Befunden mit teilweise hohem ISDS-Risiko. Insbesondere waren Kontrollen zur regelmässigen Überprüfung, Bewertung, Identifikation und Darstellung der ICT- und Datenschutz-Risiken noch nicht vollständig implementiert. Der Verwaltungsprozess der Medizintechnik und die bestehenden Verantwortlichkeiten waren noch nicht optimal abgebildet und abgestimmt, insbes. im Zusammenhang mit der Ausserbetriebnahme von Medizintechnik. Dokumentierte Vorgaben und Handlungsanweisungen bestanden nur lückenhaft. Weiter zeigte eine Schwachstellenprüfung bei den am separiertem Netzwerk angeschlossenen medizinischen Geräten Sicherheitslücken mit hoher Kritikalität. Auch die STS AG hat insoweit nur beschränkten Einfluss und ist darauf angewiesen, dass die Hersteller bzw. Lieferanten ihren Beitrag leisten (namentlich regelmässige Software-Aktualisierung für die Medizintechnik bereitstellen), damit die ISDS-Verantwortung wahrgenommen werden kann. Die DSA wird die Umsetzung von Verbesserungsmassnahmen bei der STS AG begleiten.

Spital Lindenhofgruppe AG: ICT-Grundschutz

Das Lindenhofspital ist ein privates Spital in Bern und gehört zusammen mit dem Engeried- und dem Sonnenhofspital zur Lindenhofgruppe. Diese zählt landesweit zu den führenden Listenspitälern mit privater Trägerschaft. Die Spitalgruppe bietet neben einer umfassenden interdisziplinären Grundversorgung ein Leistungen der spezialisierten und der hochspezialisierten Medizin an. Die geprüften Bereiche fokussierten sich auf die ISDS-Anforderungen im Bereich des ICT-Grundschutzes. Dieser umfasst die alle Massnahmen (Organisation, Verfahren, Hilfsmittel, Infrastruktur und technische Systeme, Daten und Vorkehrungen etc.), welche die datenschutzkonforme und sichere Abwicklung der Geschäftsprozesse, einschliesslich der Personendatenbearbeitungen, bei der Lindenhofgruppe unterstützen.

Die Prüfung ergab bei fünf von sechs primären Prüfbereichen Befunde mit mittlerem, teils aber auch hohem ISDS-Risiko. Insbesondere wurde festgestellt, dass die notwendigen Zuständigkeiten nicht eindeutig definiert waren. Dies erschwert die Einführung von Mechanismen, die nachweisbar sicherstellen, dass klassifizierte Daten ausschliesslich in Übereinstimmung mit den geltenden regulatorischen Vorgaben bearbeitet werden. Auch wurde festgestellt, dass etablierte Prozesse teilweisse nicht konsequent umgesetzt wurden. Zudem fehlten für gewisse Bereiche klare Anweisungen und Verfahren, welche die Durchführung der Prozesse steuern und erleichtern. Die DSA wird die Umsetzung von Verbesserungsmassnahmen begleiten.

VIS-Kontrolle

Die Visa-Informationssystem-Verordnung des Bundes verpflichtet die DSA zur regelmässigen Überprüfung der Zugriffe der kantonalen Behörden auf das zentrale Visa-Informationssystem der Schengen-Staaten. Erstmals prüfte die DSA im Berichtsjahr mittels einer Stichprobenkontrolle die Zugriffe durch die Mitarbeitenden des Migrationsdienstes des kantonalen Amts für Bevölkerungsdienste. Die Prüfung ergab, dass die Zugriffe im Rahmen der Aufgabenerfüllung unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgten. Gleichwohl empfahl die DSA, die Schulung und Sensibilisierung der Mitarbeitenden kontinuierlich zu stärken.

6.5 Weitere aufsichtsrechtliche Instrumente

6.5.1. Bearbeitung von Meldungen über Datenschutzvorfälle

Gestützt auf die Einführungsverordnung zur EU-Datenschutzrichtlinie 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 mehrere Datenschutzvorfälle gemeldet, die sich jeweils bei externen Leistungserbringern (namentlich Xplain AG, Concevis AG,

Unico Data AG) ereignet hatten und teils zur Folge hatte, dass Daten an Unbefugte offenbart wurden. Die auch von den Medien aufgegriffenen Vorfälle zeigten, dass die verantwortlichen Behörden bei der Auslagerung von Datenbearbeitungen ihre Verantwortung für die sorgfältige Auswahl, Instruktion und namentlich auch Kontrolle ihrer Hilfspersonen ernst nehmen müssen.

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 (Art. 15 Abs. 3 DSV).

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 Auskünfte an Gemeindebehörden 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.

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 den Einsatz von KI in der Verwaltung unter verschiedenen Gesichtspunkten (Technologie, erste praktische Anwendungen und verfassungsrechtliche Anforderungen). Privatim verfasste insgesamt 10 Stellungnahmen im Rahmen von Vernehmlassungen des Bundes, der Konferenz der Kantonsregierungen und 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 neuen Schadensorganisation Erdbeben, der Arbeitsgruppe Recht im Justizvollzug der KKJPD sowie der Körperschaft Polizeitechnik und -informatik Schweiz – leistete privatim Beratungen zur datenschutzkonformen Umsetzung der jeweiligen Vorhaben. Erneut stand privatim in regelmässigem Austausch mit dem EDÖB, namentlich zu Fragestellungen betreffend das anwendbare Datenschutzrecht und die damit verbundene Aufsichtszuständigkeit sowie zu den Datenschutzvorfällen bei IT-Dienstleistern, von denen sowohl Bundes- als auch kantonale Behörden betroffen waren (siehe Ziff. 6.5.1 oben).

Arbeitsgruppen von privatim

Die *Arbeitsgruppe Digitale Verwaltung* setzte eine Unterarbeitsgruppe zum Thema KI ein mit der Aufgabe, auf der Basis der geltenden Datenschutzgesetzgebung, unter Einbezug der Arbeiten auf EU-Ebene für eine KI-Verordnung, Grundlagen für den datenschutzkonformen Umgang mit KI zu erarbeiten und allfälligen Gesetzgebungsbedarf auszuloten.

Die *Arbeitsgruppe Sicherheit* begleitete die Arbeiten zum Vorhaben der KKJPD, ein Konkordat über den interkantonalen Datenaustausch im Polizeibereich

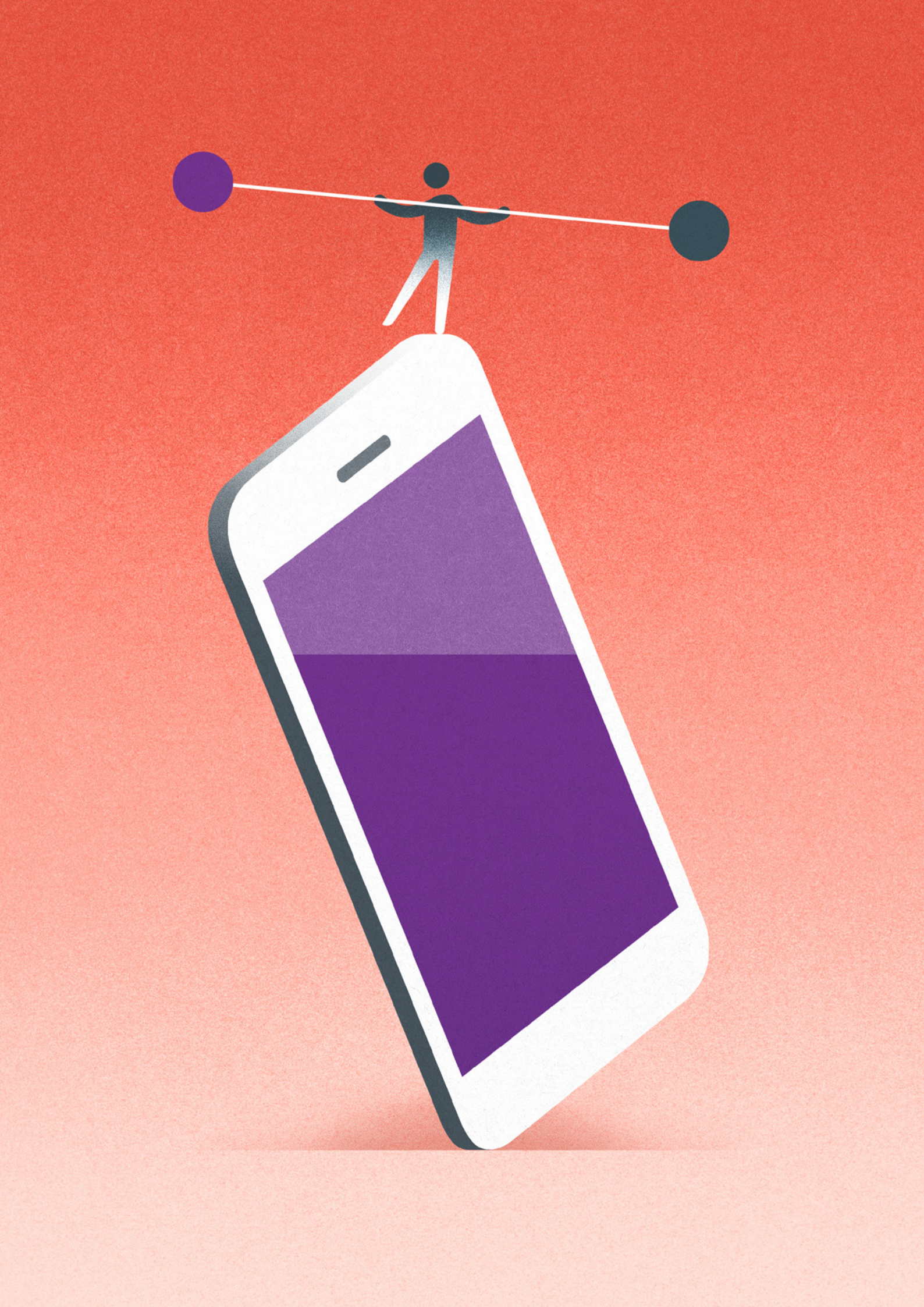
zu erarbeiten. Ein solches Konkordat wird grundsätzlich als deutlich geeigneter beurteilt als der Ansatz, in den kantonalen Polizeigesetzen einseitige Ermächtigungen zur automatisierten Bekanntgabe von Polizeidaten an andere Kantone vorzusehen. Allerdings muss ein Konkordat den vorgesehenen Datenaustausch mit genügender Bestimmtheit und auf verhältnismässige Art festlegen. Eine Blankoermächtigung, welche die Konkretisierung weitestgehend den ausführenden Organen überlässt, genügt den grundlegenden Anforderungen der Verfassung bei Grundrechtseingriffen nicht. Im Berichtsjahr nahm die Arbeitsgruppe in einer informellen Konsultation Stellung zu einem Vorentwurf und erarbeitete die Grundlagen für die formelle Stellungnahme von privatim in der von der KKJPD im November eröffneten öffentlichen Vernehmlassung.

Die Mitglieder der *Arbeitsgruppe Gesundheit* tauschten sich im Berichtsjahr unter der Leitung der stellvertretenden Datenschutzbeauftragten Recht einmal virtuell und einmal vor Ort aus. Der Austausch betraf namentlich Forschungsvorhaben und – oft damit zusammenhängend – medizinische Register: Diskutiert wurden die datenschutzrechtlichen Zuständigkeiten (kantonal und/oder eidgenössisch), das Zusammenspiel zwischen kantonalen Ethikkommissionen und Datenschutzbehörden sowie, in welchen Fällen eine Vorabkontrollpflicht besteht. Dieser Themenkomplex wird im Folgejahr weiterverfolgt, ebenso die Auseinandersetzung mit KI im Gesundheitsbereich (z. B. Radiologiebefundung mit KI-Unterstützung).

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
AG	Aktiengesellschaft
AHV	Alters- und Hinterlassenenversicherung
Art.	Artikel
AVA	Amt für Arbeitslosenversicherung
AWS	Amazon Web Services
CHF	Schweizer Franken
DSA	Datenschutzaufsichtsstelle des Kantons Bern
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
DSV	Datenschutzverordnung
DVG	Gesetz über die digitale Verwaltung
E-ArchG	Entwurf für eine Änderung des Gesetzes über die Archivierung
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EU	Europäische Union
FK	Finanzkontrolle
GERES	Gemeinderegistersystem
GSI	Gesundheits-, Sozial- und Integrationsdirektion
HIS	Harmonisierung der Informatik in der Strafjustiz
ICSG	Gesetz über die Informations- und Cybersicherheit
ICT	Informations- und Telekommunikationstechnik
IMG	Gesetz über die Information und die Medienförderung
IMV	Verordnung über die Information und die Medienförderung
IP	Internet Protocol

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
LANAT	Amt für Landwirtschaft und Natur
M365	Microsoft 365
NFFS	Neues Fallführungssystem
PolG	Polizeigesetz
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
RZ	Rechenzentrum
S.	Seite
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs
SRO AG	Spital Region Oberaargau
STA	Staatskanzlei
STS	Spital Simmental-Thun-Saanenland
SZB	Spitalzentrum Biel
TCHF	Tausend Schweizer Franken
USA	Vereinigte Staaten von Amerika
VRPG	Gesetz über die Verwaltungsrechtspflege
WLAN	Wireless Local Area Network
Ziff.	Ziffer

Datenschutzaufsichtsstelle
des Kantons Bern

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

www.be.ch/dsa