Kanton Bern
Canton de Berne

Jahresbericht Datenschutzaufsichtsstelle 2022

Datenschutzaufsichtsstelle

Februar 2023

Impressum

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

Layout und Realisation: noord.ch

Inhaltsverzeichnis

1	**Vorwort**	5
2	**Grundrecht auf Datenschutz**	6
3	**Verantwortung und Aufsicht**	8
4	**Aufgaben der Datenschutzaufsichtsstelle**	11
5	**Organisation / Ressourcen / Netzwerk**	12
6	**Fachliche Berichterstattung aus dem Arbeitsalltag**	15
6.1	Beratung	15
6.1.1	Behörden	15
6.1.2	Betroffene Personen	19
6.1.3	Weiterbildung	21
6.2	Formelle Stellungnahmen	22
6.3	Vorabkontrollen	26
6.3.1	Informatikprojekte	26
6.3.2	Videoüberwachungen	31
6.4	Audits	34
6.5	Weitere aufsichtsrechtliche Instrumente	43
6.5.1	Begründete Anträge und Beschwerdeverfahren	43
6.5.2	Oberaufsicht über die Aufsichtsstellen der Gemeinden	43
6.6	Interkantonale Zusammenarbeit	44
7	**Antrag**	46
8	**Glossar / Abkürzungen**	47

1 Vorwort

Eigentlich ist das Datenschutzrecht schnell erklärt: Wenn Behörden Personendaten bearbeiten – was bei der Erfüllung ihrer Aufgaben regelmässig geschieht –, müssen sie einige Regeln beachten und dafür sorgen, dass die Daten vor Verletzungen jener Regeln geschützt sind. Deren Zweck ist nicht, den Behörden «das Leben schwer zu machen», vielmehr geht es um ganz grundsätzliche Erwartungen im demokratischen Rechtsstaat: Wer hoheitliche Aufgaben wahrnimmt, soll sich an seine gesetzlichen Befugnisse halten (Gesetzmässigkeit) und Einschränkungen der Rechte und Freiheiten seiner Bürgerinnen und Bürger so schonend wie möglich ausgestalten (Verhältnismässigkeit). Und er muss den betroffenen Personen offenlegen, welche Daten er über sie zu welchen Zwecken bearbeitet (Transparenz).

Was zunächst klar und selbstverständlich klingt, wird ungleich anspruchsvoller, wenn es darum geht, die wenigen Grundsätze auf die Vielfalt der Fragestellungen im Behördenalltag anzuwenden. Darf die Verwaltung sämtliche Daten in ihrer elektronischen Geschäftsverwaltung in das Testsystem kopieren, um dort neue Funktionen zu prüfen und Schulungen durchzuführen? Ist es ihr erlaubt, unaufgefordert SMS an Arbeitslose zu senden, um sie an den bevorstehenden Termin beim Arbeitsvermittlungszentrum zu erinnern? Ist es verhältnismässig, wenn die verantwortliche Behörde in einem Rückkehrzentrum Videokameras installiert, um in der Nacht und an Wochenenden die Sicherheit mit weniger Personal gewährleisten zu können? Und hat eine Person Anspruch darauf, die Akten einzusehen, die das zuständige Amt bei der Abklärung der Fahrtüchtigkeit ihres inzwischen verstorbenen Vaters erstellt hat?

Zwar ist jede Behörde stets selbst dafür verantwortlich, dass sie bei der Bearbeitung von Personendaten die rechtsstaatlichen Grundsätze befolgt und die Sicherheit der Daten gewährleistet. Von ihr wird aber nicht erwartet, dass sie jede datenschutzrechtliche Fragestellung alleine löst, vor allem wenn sich die Frage zum ersten Mal stellt. Es ist bereits viel gewonnen, wenn die Behörde schon nur erkennt, dass eine Situation datenschutzrechtlich relevant ist, und bei der zuständigen Datenschutzaufsichtsstelle oder einer anderen dafür bezeichneten Anlaufstelle Rat sucht.

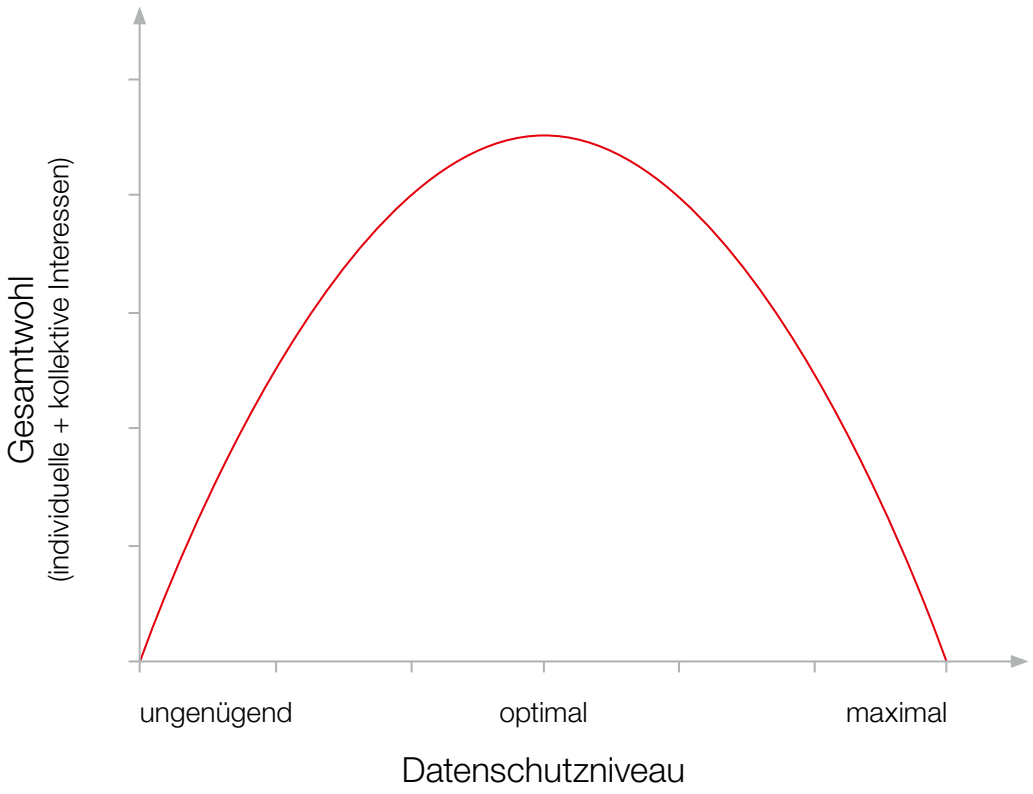
Der vorliegende Bericht vermittelt einen Einblick in die Breite der behördlichen Tätigkeiten, bei welchen sich Datenschutzfragen stellten, mit denen die DSA im Rahmen ihrer Beratungs- und Aufsichtsaufgaben im Berichtsjahr befasst wurde.

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.

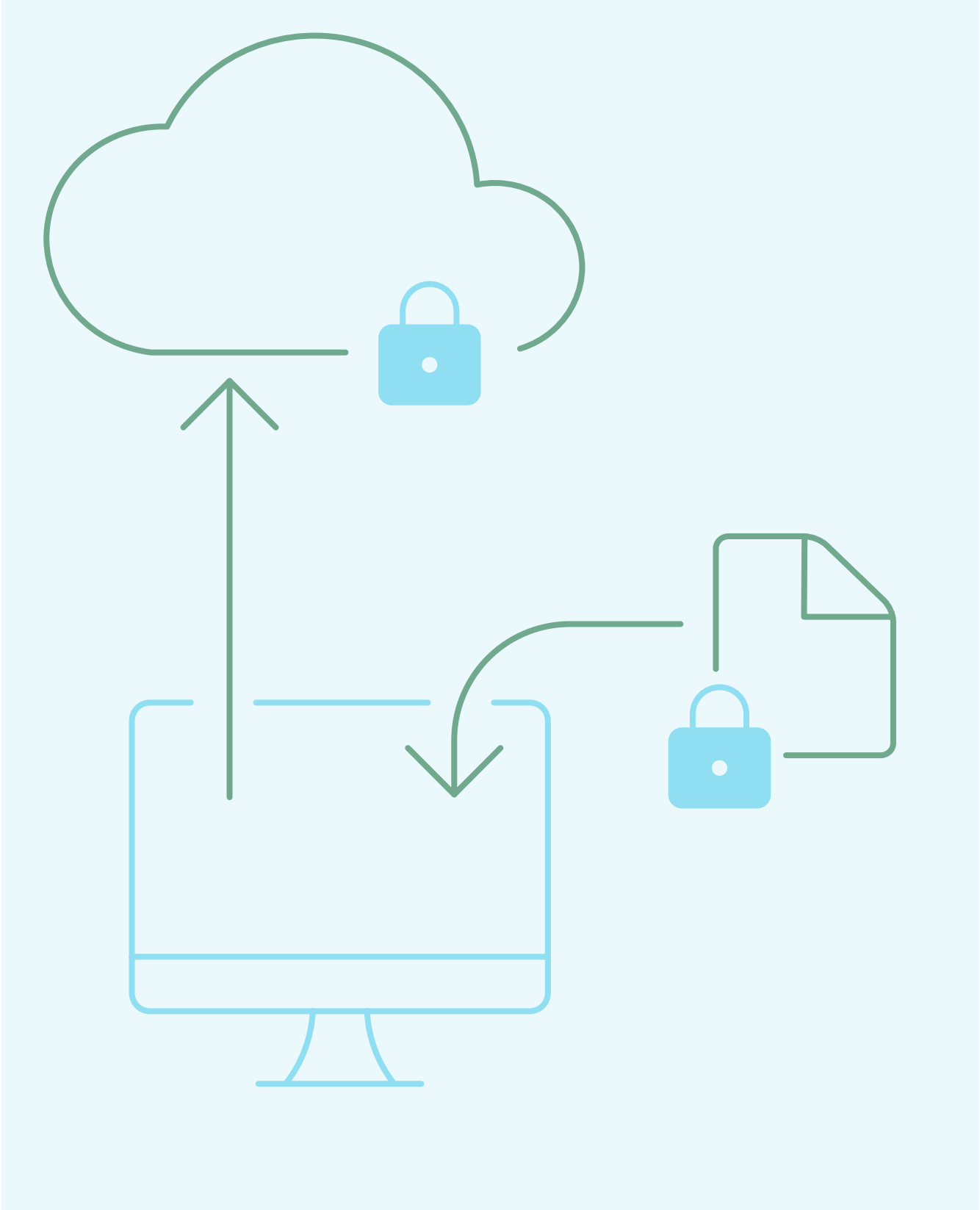
Das Datenschutzgesetz (KDSG) konkretisiert die Pflichten der Behörden beim Bearbeiten von Personendaten, wobei nebst der Verwaltung auch weitere Träger von öffentlichen Aufgaben, z. B. Schulen und Spitäler, als Behörden gelten. Dabei umfasst «Bearbeiten» jeden Umgang mit Personendaten, wie das Beschaffen, 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.

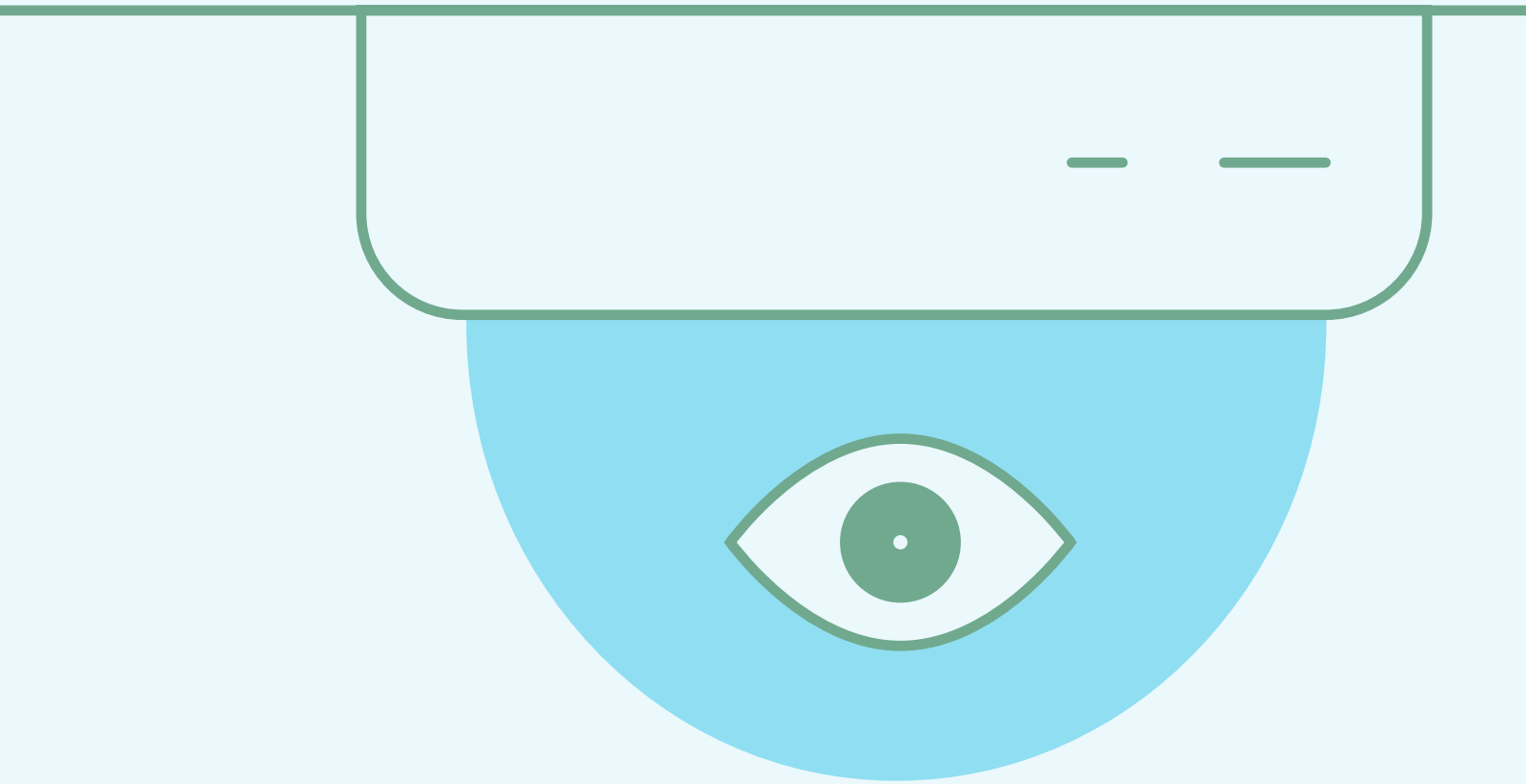
3 Verantwortung und Aufsicht

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 kantonale Datenschutzaufsichtsstelle (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 gehört die BLS AG zurzeit zwar mehrheitlich dem Kanton Bern, die Konzession für die Personenbeförderung erhält sie jedoch im Rahmen dessen Monopols vom Bund. Ihre Datenbearbeitungen z. B. im Rahmen einer Ticketing-App unterstehen deshalb dem DSG und der Aufsicht des EDÖB. Umgekehrt untersteht der Vollzug von Bundesgesetzen – z. B. des Epidemiengesetzes (EpG) – durch die kantonalen Behörden dem Datenschutzrecht des jeweiligen Kantons.





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 2022 verfügte die DSA über einen Personalbestand von 570 %, aufgeteilt auf sieben Personen. Davon sind fünf Personen juristisch ausgebildet, zwei Personen sind Informatiker bzw. Informatikprüfer:

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

Anders Bennet (stv. 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 (stv. Datenschutzbeauftragte Recht) ist Rechtsanwältin und arbeitet seit 2009 bei der DSA. Sie leitet seit 2012 den Fachbereich Gesundheit + Bildung und betreut die Gesundheits-, Sozial- und Integrationsdirektion (GSI) sowie die Bildungs- und Kulturdirektion (BKD) in datenschutzrechtlichen Fragen. In Vorabkontrollen prüft sie die eingereichten ISDS-Dokumente hinsichtlich rechtlicher Aspekte.

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

Stephanie Siegrist (Wissenschaftliche Mitarbeiterin Recht) ist Juristin und Historikerin und arbeitet seit 2021 bei der DSA. Sie ist im Fachbereich Gesundheit + 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 arbeitet im Fachbereich Gesundheit + Bildung und betreut Auskunfts- und Beratungsgeschäfte, Vorabkontrollen sowie Stellungnahmen zu Erlassen, die den Datenschutz betreffen.

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

Angesichts der weiterhin stark zunehmenden Arbeitslast insbesondere im Bereich der Vorabkontrollen (siehe dazu Ziff. 6.3) hat die DSA dem Grossen Rat im Rahmen des Voranschlags 2023 den Antrag auf Schaffung einer zusätzlichen Vollzeitstelle unterbreitet, was vom Parlament bewilligt wurde. Ein Workshop zur Arbeitszufriedenheit und Gesundheit der Mitarbeitenden ergab, dass diese gerne für die DSA arbeiten und die gelebte Kultur sehr schätzen, dass jedoch auch weitere Massnahmen erarbeitet werden müssen, um die vorhandenen Kräfte und die Arbeitsmenge in einem gesunden Gleichgewicht zu halten.

Im Jahr 2022 betrug der Betriebsaufwand der DSA insgesamt TCHF 210. Davon wurden ca. 75 % (TCHF 157) für externe Dienstleistungen zur Unterstützung von Informatikprüfungen eingesetzt. Weil drei Rechnungen des Vorjahres über total TCHF 69 nach einem Versehen erst im Jahr 2022 verbucht werden konnten, weist die DSA in der Staatsrechnung 2022 des Kantons Bern einen Betriebsaufwand von TCHF 279 aus und überschreitet das Budget um insgesamt TCHF 55.

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 einen IT-Sicherheitsverantwortlichen. Die Gemeindebehörden können sich mit allgemeinen Datenschutzfragen an das Amt für Gemeinden und Raumordnung (AGR) 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 2022 führte sie ein erstes gemeinsames Treffen und einen Folgeanlass mit allen Kontaktstellen für Datenschutz durch, um den Austausch mit und auch unter diesen zu verstärken. Zudem pflegt sie institutionalisierte Kontakte zu Behörden, bei deren Tätigkeiten sich regelmässig anspruchsvolle datenschutzrechtliche Fragen stellen (Beispiele: Amt für Informatik und Organisation [KAIO], Bedag AG, Kantonspolizei [KAPO] und Insel Gruppe AG).

Im Hinblick auf einen gesamtstaatlich abgestimmten ISDS-Auditplan pflegen 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 Fachbereichsleiterin Gesundheit + Bildung 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

Nutzung von Cloud-Services durch kantonale Behörden

Im Februar des Berichtsjahres verabschiedete privatim eine neue Fassung des Merkblatts «Cloud-spezifische Risiken und Massnahmen». Namentlich bei internationalen Cloud-Anbietern mit technisch, organisatorisch und rechtlich weitestgehend standardisierten Leistungsangeboten verliert die Behörde die tatsächliche Kontrolle darüber, welche von ihr zu schützende Daten (inkl. solche über die Nutzerinnen und Nutzer der Cloud-Dienste) wo (geografisch) zu welchen Zwecken bearbeitet werden und wer alles (inkl. Subunternehmen) Einsicht in jene nehmen kann. Entsprechend hoch sind die Risiken für die Vertraulichkeit der Daten, erst recht falls der Cloud-Anbieter wegen seines Auslandsbezugs verpflichtet werden kann, Daten an fremde Behörden herauszugeben. In einem Beschluss vom März 2022 über die Zulassung von Microsoft 365 (M365) befasste sich der Regierungsrat des Kantons Zürich fast ausschliesslich mit diesem letzten Risiko (sog. «lawful access») und erachtete es im konkreten Fall als vernachlässigbar; die Aspekte der Lieferantenabhängigkeit und des Kontrollverlusts bezeichnete er als unvermeidbar. Er beschloss deshalb, die Cloud-Lösung M365 in der kantonalen Verwaltung zuzulassen, gleichzeitig hielt er aber fest, dass die einzelnen Verwaltungseinheiten weiterhin für den Datenschutz verantwortlich seien und die Direktionen und die Staatskanzlei bei Bedarf zusätzliche Regelungen erlassen müssten, um einen rechtskonformen Einsatz von M365 zu gewährleisten.

Für den Kanton Bern, der die Einführung von M365 als Teil der Grundversorgung der Kantonsverwaltung ebenfalls prüft, hat die DSA – entsprechend dem Cloud-Merkblatt von privatim – dem Regierungsrat und dem federführenden KAIO ein anderes Vorgehen empfohlen: Auf der Grundlage einer umfassenden Risikoanalyse, welche sich mit sämtlichen Risiken für alle betroffenen Personen befasst und auch ein Ausstiegsszenario enthält, sind alle technischen und organisatorischen Massnahmen zu definieren, welche für einen datenschutzkonformen und sicheren Einsatz der einzelnen Services erforderlich sind. Die als tragbar erachteten Restrisiken sind dem Regierungsrat vollständig und transparent auszuweisen, der diese akzeptieren und dafür die Verantwortung

übernehmen soll. Im Berichtsjahr beriet die DSA das KAIO bei der (nach wie vor laufenden) Erarbeitung des Risikoberichts an den Regierungsrat.

Als Präsident von privatim war der Leiter der DSA massgeblich an der Beratung der Schweizerischen Informatikkonferenz (SIK) beteiligt, welche ihren Rahmenvertrag mit Microsoft über die Nutzung von Online-Services durch schweizerische öffentliche Organe für die Dauer vom 1. Mai 2022 bis 30. April 2025 erneuerte. Über die bereits im Herbst 2020 ausgehandelte Vereinbarung über die Anwendung des schweizerischen Rechts und die schweizerische Gerichtsbarkeit für Klagen zur Durchsetzung der vertraglichen Datenschutzversprechen von Microsoft hinaus konnten weitere Klärungen und Zusagen zum Schutz der Vertraulichkeit der Daten erreicht werden. Nichts desto trotz verbleiben einige vertragliche Risiken und vor allem der tatsächliche Kontrollverlust betreffend die ausgelagerten Daten, weshalb eine umfassende Risikobeurteilung unverzichtbar ist.

In einer anders gelagerten Beratung war die Spital Region Oberaargau (SRO) AG dagegen nicht für den Datenschutz in der Cloud verantwortlich: Ein Hausarzt wollte der SRO AG medizinische Berichte zur konsiliarischen Beratung mittels einer Cloud-Plattform zugänglich machen, wobei die SRO AG ihre Konsiliarberichte weiterhin auf den herkömmlichen Kanälen versandte. Hier oblag die Datenschutzverantwortung für den Cloud-Service dem Hausarzt. Die DSA empfahl der SRO AG immerhin zu überprüfen, dass der Dokumentenabruf aus der Cloud keine Sicherheitsrisiken für ihre eigenen Systeme brachte.

Systematische Verwendung der AHV-Nummer ausserhalb der AHV

Anfangs 2022 trat eine Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) in Kraft, wonach die Einheiten der Kantons- und Gemeindeverwaltungen die AHV-Nummer systematisch verwenden dürfen, soweit sie zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Die Verwendung der AHV-Nummer gilt als systematisch, wenn sie zusammen mit anderen Personendaten in einer Datensammlung geführt wird. Für die vom Gesetz verlangte Erforderlichkeit genügt es nicht, dass es praktisch ist, die AHV-Nummer zu verwenden; vielmehr muss ein nachvollziehbares fachliches Bedürfnis – namentlich die Qualitätssicherung und Effizienzsteigerung bei automatisierten Datenbearbeitungen – bestehen, welches ohne Gebrauch der AHV-Nummer nur ungenügend bedient werden kann. Mit der Erlaubnis zur systematischen Verwendung der AHV-Nummer gehen mehrere Pflichten der berechtigten Behörden einher: Diese müssen die gesetzlich vorgesehenen technischen und organisatorischen Massnahmen zum Schutz der Nummer vor Missbräuchen treffen (Art. 153*d* AHVG) und die Zentrale Ausgleichsstelle über die Verwendung informieren (Art. 153*f* AHVG). Der Kanton als Ganzes muss periodisch eine Risikoanalyse durchführen, die insbesondere dem Risiko einer unerlaubten Zusammenführung von Datenbanken Rechnung trägt. Hierfür ist ein Verzeichnis der Datenbanken zu führen, in denen die AHV-Nummer systematisch verwendet

wird (Art. 153*e* AHVG). Im Juli des Berichtsjahres machte die DSA die Direktionen und die Staatskanzlei auf die gesetzlichen Pflichten aufmerksam, im Dezember gelangte sie an die einzelnen Verwaltungseinheiten, damit diese zurückmelden, ob sie die AHV-Nummer systematisch verwenden, und gegebenenfalls Bericht über die getroffenen Massnahmen erstatten.

SMS-Dienst für arbeitslose Personen

Das Amt für Arbeitslosenversicherung (AVA) gelangte an die DSA, weil es für seine Kundinnen und Kunden einen SMS-Dienst einrichten wollte, um sie per SMS an die für Kontaktaufnahmen angegebene Mobiltelefonnummer an bevorstehende Beratungsgespräche beim Arbeitsvermittlungszentrum erinnern und über erfolgte Auszahlungen der Arbeitslosenkasse informieren zu können. Die DSA beurteilte das Vorhaben grundsätzlich als zulässig, weil die Verwendung der Mobilnummer im Bereich der gesetzlichen Aufgaben des AVA und zudem im mutmasslichen Interesse der betroffenen Personen lag. Sie empfahl aber, eine Widerspruchsmöglichkeit vorzusehen und den Versand einzustellen, wenn sich eine Person nach Erhalt der SMS ausdrücklich dagegen ausspricht («opt out»). Zudem riet sie wegen der Möglichkeit, dass unbeteiligte Dritte Einsicht in die SMS erhalten, einen neutralen Text zu wählen, der keine Rückschlüsse auf die Absenderin bzw. die Arbeitssituation der betroffenen Person zulässt.

Rechtsgrundlage für Internet-Veröffentlichungen

Das AGR unterbreitete der DSA die Frage, ob es genüge, wenn das Geschäftsreglement einer Regionalkonferenz die Veröffentlichung von Versammlungsprotokollen im Internet vorsehe, oder ob dafür eine Verordnung erforderlich sei. Regionalkonferenzen sind öffentlich-rechtliche Körperschaften im Sinne des Gemeindegesetzes und ihre Protokolle müssen – wie jene von Gemeindeversammlungen – öffentlich sein. Für die Veröffentlichung im Internet braucht es aktuell jedoch eine besondere Vorschrift, die dies erlaubt (Art. 2 Datenschutzverordnung [DSV]). Die Regionalkonferenzen regeln die Erfüllung ihrer Aufgaben durch Reglement und können dort alle zur Aufgabenerfüllung erforderlichen Vorschriften erlassen, soweit die kantonale Verordnung über das Geschäftsreglement für die Regionalkonferenzen dafür Raum lässt. Vor diesem Hintergrund hielt die DSA die Vorschrift im Geschäftsreglement für genügend, zumal dieses dem fakultativen Referendum untersteht.

Die im Herbst 2022 vom Grossen Rat verabschiedete Änderung des Informationsgesetzes (neu: Gesetz über die Information und die Medienförderung, IMG) bringt eine Rechtsgrundlage für alle kantonalen und kommunalen Behörden. Diese werden neu im Rahmen von Informationen von allgemeinem Interesse auch Personendaten im Internet veröffentlichen dürfen, soweit nicht überwiegende

öffentliche oder private Interessen entgegenstehen (Art. 15b in Verbindung mit Art. 16 Abs. 1 Bst. a und c IMG).

Auswertung von Logdaten bei Missbrauchsverdacht

Die Steuerverwaltung des Kantons Bern (SV) wollte sichergehen, dass Mitarbeitende im Falle einer Auswertung von Logdaten zur Kontrolle von Ausstandspflichten vorab darüber informiert werden müssen. Die DSA bestätigte diese Annahme: Das Personalgesetz (PG) und die Randdatenverordnung (RDV) regeln die Voraussetzungen und den Prozess für die Auswertung von Logdaten streng und ausführlich. Eine personenbezogene, namentliche Auswertung im Zusammenhang mit einem möglichen Missbrauch ist nur dann zulässig, wenn ein konkreter Verdacht vorliegt oder ein Missbrauch bereits erwiesen ist (Art. 12d Abs. 3 PG). Zudem muss die betroffene Person über den Verdacht oder Missbrauch schriftlich informiert worden sein (Art. 12d Abs. 4 PG). Die mit der Auswertung beauftragte Behörde muss schliesslich diese Voraussetzungen prüfen, bevor sie die Auswertung durchführt (Art. 11 RDV).

Datenschutzlexikon für die Volksschule

Für den Datenschutz in der bernischen Volksschule verfasste das Amt für Kindergarten, Volksschule und Beratung (AKVB) im Jahr 2008 einen Datenschutzleitfaden. Da dieser inzwischen ziemlich in die Jahre gekommen ist, überarbeitet ihn das AKVB seit Sommer 2020. Die neue Fassung soll als «Datenschutzlexikon» im Jahr 2023 verabschiedet werden.

Die DSA begleitete das Projekt im Rahmen ihres Beratungsauftrags aktiv und liess die neusten datenschutzrechtlichen Erkenntnisse insbesondere zu den Cloud-spezifischen Risiken und Massnahmen in die Projektgruppe einfliessen. Das neue Datenschutzlexikon soll den Volksschulen als erste Anlaufstelle für datenschutzrechtliche Fragestellungen im Sinne der «Hilfe zur Selbsthilfe» dienen, sie für das Thema sensibilisieren und damit die datenschutzrechtlichen Kompetenzen an der Volksschule fördern.

Umgang mit der Behandlungsdokumentation nach Aufgabe einer Arztpraxis

Ein Spital mit einem Leistungsauftrag des Regierungsrats (sog. Listenspital) fragte die DSA an, wie es mit den Behandlungsdokumentationen nach Aufgabe der Praxistätigkeit eines Hausarztes umzugehen habe.

Die DSA wies das Listenspital auf Artikel 26 des Gesundheitsgesetzes hin. Danach hat die Fachperson auch nach Aufgabe ihrer Praxistätigkeit zu gewährleisten, dass die Behandlungsdokumentation unter Wahrung der Schweigepflicht verwaltet und den berechtigten Patientinnen und Patienten der Zugang dazu ermöglicht wird (Abs. 3). Weitergehende Bearbeitungen der Behandlungsdokumentation sind nicht erlaubt. Als Aufbewahrungsstelle kommt namentlich eine Person in Betracht, die derselben beruflichen Schweigepflicht untersteht, also eine andere Arztperson. Dafür benötigt sie die Einwilligung der betroffenen Patientinnen und Patienten nicht. Gestützt auf eine schriftliche Vereinbarung mit der Patientin oder dem Patienten kann sie sich von ihrer Aufbewahrungspflicht allerdings befreien, indem sie die Behandlungsdokumentation der nachbehandelnden Fachperson oder der Patientin oder dem Patienten selbst übergibt (Abs. 4).

6.1.2. Betroffene Personen

Zuständigkeit für Auskunftsgesuche in Steuersachen

Eine Person bat die DSA um Unterstützung bei ihrem Auskunftsgesuch zu ihren Steuerdaten eines bestimmten Veranlagungsjahrs. Zunächst stellte sich die Frage, welche Steuerbehörde für das Gesuch zuständig ist. Die Abklärung ergab, dass unabhängig davon, ob ein Gesuch bei einer der fünf regionalen oder einer der drei städtischen Steuerbehörden (Bern, Biel, Thun) eingereicht wird, eine Stelle der kantonalen Steuerverwaltung für die Bearbeitung sämtlicher Auskunftsgesuche zuständig ist. Die regionalen und städtischen Steuerbehörden sind entsprechend instruiert, eintreffende Gesuche unverzüglich weiterzuleiten. Bürgerinnen und Bürger können somit ohne Nachteil ein Gesuch bei einer der Steuerbehörden einreichen.

Einsicht in Daten verstorbener Personen

Eine Person hatte beim Strassenverkehrs- und Schifffahrtsamt (SVSA) um Einsicht in die Akten zur Abklärung der Fahrtüchtigkeit ihres inzwischen verstorbenen Vaters ersucht, was vom SVSA unter Verweis auf den Datenschutz abgelehnt wurde. Die DSA konnte die ratsuchende Person auf eine Vorschrift in der Datenschutzverordnung hinweisen: Danach ist die Auskunft über Daten von verstorbenen Personen zu erteilen, wenn die Gesuchstellerin oder der Gesuchsteller ein Interesse an der Auskunft nachweist – was bei naher Verwandtschaft als gegeben gilt – und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen (Art. 12 DSV). Mit dieser Auskunft war die Person in der Lage, dem SVSA darzulegen, dass das Datenschutzrecht die erbetene Einsicht nicht nur nicht verbietet, sondern sogar ausdrücklich erlaubt.

Datenschutzverletzung durch Absenderangabe auf Postsendung?

Eine Person hatte von der KAPO eine Ordnungsbusse per Post erhalten, wobei auf dem Umschlag der Absender «POLICE Bern» ersichtlich war. Sie sah darin eine Datenschutzverletzung und wandte sich an die DSA, welche ihr wie folgt Auskunft gab: Aus der Nennung des Absenders auf Postversänden des Kantons Bern ist tatsächlich ersichtlich, dass die Empfängerin oder der Empfänger mit der betreffenden Verwaltungseinheit in irgendeiner Form zu tun hat. Allerdings sind die möglichen Gründe für einen Behördenkontakt und einen daraus resultierenden Postversand so vielfältig, dass auf dem Briefumschlag nicht mehr ersichtlich ist als die Tatsache, dass die betroffene Person von der genannten Stelle Post erhält. Im Falle der KAPO ist es z. B. möglich, dass die Person eine Sicherheitsberatung zum Einbruchsschutz gewünscht, der KAPO eine Veranstaltung (wie einen 1. Augustumzug) gemeldet oder sich nach einem Aufruf als Zeugin eines Vorfalls gemeldet hat und nun zur Befragung eingeladen wird. Die blosse Erkennbarkeit des Absenders für das Postpersonal – welches im Falle der Nichtzustellbarkeit wissen muss, an wen der Versand zu retournieren ist, ohne dass der Umschlag dafür zu öffnen ist – lässt deshalb in der Regel keine weitergehenden Schlüsse zu und ist somit als zulässig zu erachten.

Dies schliesst jedoch nicht aus, dass in besonders gelagerten Fällen eine Rechtsverletzung besteht: So lässt der Versand einer Behörde wie der Rekurskommission des Kantons Bern für Massnahmen gegenüber Fahrzeugführerinnen und Fahrzeugführern sehr viel konkretere Schlüsse über den Inhalt des Versands und damit über die Empfängerin oder den Empfänger zu. Gelten – wie beim Bund – Daten über verwaltungsrechtliche Sanktionen künftig als besonders schützenswerte Personendaten, deren Bekanntgabe an Dritte nur bei zwingender Notwendigkeit erlaubt ist, so dürfte im genannten Beispiel eine vollständige Absenderangabe kaum zulässig sein, solange als Absender eine Abkürzung und eine Postfachadresse angegeben werden können.

Datenschutz im Mehrparteien-Verwaltungsverfahren (z. B. Planerlassverfahren)

Auf eine aufsichtsrechtliche Anzeige in einem Strassenplanverfahren hin prüfte die DSA, inwieweit die instruierende Behörde – namentlich im Rahmen ihrer Verfügung – in einem erstinstanzlichen Mehrparteienverfahren Angaben über eine Partei an die anderen Parteien bekanntgeben darf. Einerseits haben die Parteien nach dem Gesetz über die Verwaltungsrechtspflege (VRPG) grundsätzlich Anspruch auf Einsicht in alle Verfahrensakten, andererseits gilt jedoch auch das KDSG, wonach die Bekanntgabe von Personendaten an private Dritte nur insoweit erlaubt ist, als es für die Aufgabenerfüllung notwendig ist. Ob es notwendig ist, dass eine Partei auch die Identitäten und Anliegen aller anderen Parteien kennt, auch wenn diese nichts mit den eigenen Interessen zu tun haben, liegt nicht auf der Hand.

Rechtspolitisch erkennt die DSA sachliche Gründe für die Zulässigkeit einer solchen Bekanntgabe. Namentlich bei Einsprachen, mit denen die Verletzung des öffentlichen Rechts gerügt werden kann, fördert die gegenseitige Offenlegung der Einsprechenden und deren Vorbringen die Qualität der Einsprachen, allfälliger Rechtsmittel und damit letztlich auch des behördlichen Entscheids. Zudem sind Aspekte der Verfahrensökonomie zu beachten: Dürften die Einsprechenden nichts voneinander wissen, müsste die instruierende Behörde ihre Verfahrens- und Endverfügungen individuell anonymisieren (schwärzen). Bei Verfahren mit sehr vielen Parteien würde ein unverhältnismässiger Aufwand entstehen, der sich kaum mehr mit dem Schutz der Privatsphäre rechtfertigen liesse. Die DSA wird deshalb in der laufenden Revision des VRPG den Antrag stellen, die Rechtslage zu klären und die Offenlegung soweit zu legitimieren, als nicht überwiegende Geheimhaltungsinteressen bestehen.

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 Redner/innen 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.

Wissensvermittlung im Rahmen von spezifischen Anlässen

Der Datenschutzbeauftragte nahm auf Anfrage an verschiedenen Fachkonferenzen und Weiterbildungsanlässen teil und referierte dabei über die aktuellen Herausforderungen der Datenschutzbehörden (Anlass zum internationalen Datenschutztag der Universität Lausanne), die Auftragsdatenbearbeitung durch Cloud-Anbieter (Gastvortrag im Rahmen der Vorlesung «Datenschutzrecht» der Universität Luzern, 26. Symposium on Privacy and Security sowie Workplace Conference 2022 der SIK) und über den Datenschutz bei der digitalen Transformation im Schulwesen (Tagung der Pädagogischen Hochschule Bern).

6.2 Formelle Stellungnahmen

Totalrevision des Datenschutzgesetzes

Das aus dem Jahre 1986 stammende KDSG soll an die technische Entwicklung und neuen Vorgaben im europäischen Recht – namentlich die Richtlinie (EU) 2016/680 über den Datenschutz im Strafbereich und die Änderung der Datenschutzkonvention des Europarats – angepasst werden. Gestützt auf den im August 2020 von der Direktorin DIJ an das Rechtsamt erteilten Gesetzgebungsauftrag nahm die DSA in zwei direktionsübergreifenden Arbeitsgruppen («Europäisches Recht» und «politische Fragen») Einsitz und brachte ihre Anliegen und Beurteilungen in das Vorhaben ein. Im Berichtsjahr fand nun das erste Mitberichtsverfahren zum Vernehmlassungsentwurf für das totalrevidierte KDSG statt. Zur seit den Sitzungen der Arbeitsgruppen noch einmal erheblich überarbeiteten Vorlage brachte die DSA zahlreiche teils gesetzestechnische und teils wichtige inhaltliche Hinweise an.

Zu diesen Hinweisen gehörte der Antrag, auf eine neue Bestimmung zu verzichten, wonach Behörden Personendaten auch ohne gesetzliche Grundlage bearbeiten dürfen, wenn die betroffene Person in die Bearbeitung eingewilligt oder ihre Daten allgemein zugänglich gemacht hat. Das verfassungsmässige Legalitätsprinzip verlangt für jede Personendatenbearbeitung eine Rechtsgrundlage. Eine Datenbearbeitung erfolgt nie zum Selbstzweck, sondern stets zur Erfüllung einer gesetzlichen Aufgabe, für die ihrerseits eine gesetzliche Grundlage bestehen muss, andernfalls ist das Legalitätsprinzip verletzt. Auch verlangt das Verhältnismässigkeitsprinzip, dass die Datenbearbeitung für die jeweilige Aufgabenerfüllung notwendig ist. Diesfalls genügt bereits heute eine hinreichend bestimmte Aufgabennorm, damit die betreffenden Datenbearbeitungen legitimiert sind (sog. indirekte Rechtsgrundlage). Hat die betroffene Person ihre Daten allgemein zugänglich gemacht, mag dies die verantwortliche Behörde davon befreien, die Daten bei der betroffenen Person zu beschaffen. Auch dann kann die Behörde jedoch nicht jegliche Daten (allenfalls sogar nur auf Vorrat) beschaffen und weiterbearbeiten, sondern nur jene, die für eine gesetzlich vorgesehene Aufgabe erforderlich sind. Die Erlaubnis von Datenbearbeitungen ohne gesetzliche Grundlage verspricht mehr, als sie angesichts des Legalitäts- und des Verhältnismässigkeitsprinzips tatsächlich ermöglicht, und birgt deshalb die Gefahr von unzulässigen Datenbearbeitungen durch die Behörden.

Weiter beantragte die DSA, die Verantwortung für den Datenschutz weiterhin der Behörde zuzuweisen, «die die Personendaten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeitet oder bearbeiten lässt». Zwar hat die aus dem europäischen Recht übernommene und im revidierten DSG verwendete Formulierung «wer über den Zweck und die Mittel der Datenbearbeitung entscheidet» auch vorübergehend Eingang in das neue Gesetz über die digitale Verwaltung (DVG) gefunden. Es ist jedoch zu beachten, dass die Formulierung sowohl auf europäischer

als auch auf Bundesebene immer auch für private Datenbearbeiter gilt und darum generisch gefasst sein muss. Im ausschliesslich für behördliche Datenbearbeitungen geltenden KDSG kann und muss die Verantwortung nach wie vor daran anknüpfen, wer als Träger der öffentlichen Aufgabe die Verfassungsmässigkeit der dazu erforderlichen Datenbearbeitungen gewährleisten muss. Mit der bisherigen Vorschrift wird dies – auch mit Blick auf die Unterscheidung, ob eine öffentliche Aufgabe übertragen wird (so dass der Empfänger selbst zur verantwortlichen Behörde wird) oder ob eine Hilfsperson als Auftragsbearbeiterin beigezogen wird (so dass die Verantwortung bei der ursprünglichen Behörde verbleibt) – unmissverständlich festgehalten.

Gesetz über die Informations- und Cybersicherheit

Wer Personendaten bearbeitet, muss mit geeigneten technischen und organisatorischen Massnahmen für deren Sicherheit – d. h. die Vertraulichkeit, die Integrität und die Verfügbarkeit der Daten – sorgen. Allerdings weisen nicht nur Personendaten einen besonderen Schutzbedarf auf, sondern auch sachbezogene Informationen, welche zur Wahrnehmung der öffentlichen Aufgaben benötigt werden. Das Gesetz über die Informations- und Cybersicherheit (ICSG) soll die Rahmenbedingungen definieren, damit die Behörden die sichere Bearbeitung von Informationen und den sicheren Einsatz von ICT-Mitteln gewährleisten. Wie bei der KDSG-Revision nahm die DSA auch an den direktionsübergreifenden Vorarbeiten für das neue ICSG aktiv teil. Der im ersten Mitberichtsverfahren vorgelegte Vernehmlassungsentwurf war entsprechend ausgereift, so dass die DSA primär gesetzestechnische Hinweise anzubringen hatte, welche von der federführenden FIN fast vollständig übernommen wurden.

Aus inhaltlicher Sicht erachtete es die DSA als wichtig, dass das ISCG (wie das entsprechende Bundesgesetz) eine Vorschrift zum Umgang mit den Risiken für die Informationssicherheit enthält. Die Behörden sind demnach zu verpflichten, dass sie diese Risiken laufend beurteilen und die erforderlichen Massnahmen treffen, um die Risiken zu vermeiden oder auf ein tragbares Mass zu reduzieren. Risiken, die getragen werden sollen, sind nachweislich zu akzeptieren. Auch dieses Anliegen fand Eingang in den Vorentwurf für die Vernehmlassung (Art. 5 Abs. 2 VE-ICSG).

Änderung des Polizeigesetzes

Im Nachgang zur Aufhebung einzelner Bestimmungen durch das Bundesgericht soll das per 2020 totalrevidierte Polizeigesetz (PolG) erneut revidiert werden. Im Rahmen des ersten Mitberichtsverfahrens und der anschliessenden öffentlichen Vernehmlassung brachte die DSA folgende zwei Hauptkritikpunkte an: Zum einen soll es bei der automatisierten Fahrzeugfahndung und Verkehrsüberwachung (AFV) – d. h. beim elektronischen Erfassen von Kontrollschildern und Abgleichen

mit polizeilichen Datenbanken – neu möglich sein, auch die Daten ohne Treffer («no hits») während 100 Tagen aufzubewahren und für spätere Suchläufe zu verwenden. Wenn wie geplant 22 ortsfeste AFV-Anlagen beschafft und diese an stark befahrenen Standorten wie dem Grauholz installiert werden, wo täglich über 100 000 Fahrzeuge passieren, so würde ein permanenter Datenbestand von mehreren 100 Millionen Datensätzen entstehen – um vielleicht in den nächsten 100 Tagen einen weiteren Treffer erzielen zu können. Die massenhafte Vorratsdatenspeicherung von Daten unbescholtener Bürgerinnen und Bürger sowie deren zukünftige permanente Kontrolle wären aus Sicht der DSA ein gefährlicher Schritt hin zu einem Überwachungsstaat und selbst bei Schaffung einer Gesetzesgrundlage als unverhältnismässig und damit verfassungswidrig zu bewerten. Dass der Revisionsentwurf auf einer Vorlage der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) beruht, vermag daran nichts zu ändern.

Zum anderen besteht unbestrittenermassen das berechtigte Bedürfnis, die Zusammenarbeit der kantonalen Polizeikorps – und dabei auch den Austausch von polizeilichen Daten – zu verstärken. Der richtige Weg dazu führt über ein Konkordat, in dem die gemeinsam wahrgenommenen Aufgaben hinreichend bestimmt umschrieben und die Trägerschaft dieser Aufgaben festgelegt werden; gleichzeitig können einheitliche Regelungen über die bearbeiteten Personendaten und die Zugriffe auf diese definiert sowie das anwendbare Datenschutzrecht und die zuständige(n) Aufsichtsbehörde(n) benannt werden. Die KKJPD hat deshalb ein Projekt zur Erarbeitung eines solchen Konkordats eröffnet, welches von privatim fachlich begleitet wird (siehe dazu Ziff. 6.6 unten). Zur Beschleunigung des Datenaustauschs sollen nun aber – ebenfalls auf Vorschlag der KKJPD – die Kantone in ihren Polizeigesetzen die einseitige Ermächtigung vorsehen, um den anderen Kantonen ihre polizeilichen Informationssysteme im Abrufverfahren zugänglich zu machen. Die DSA hält eine solche einseitige Ermächtigung jedoch für verfassungswidrig: Wenn Artikel 28 der Kantonsverfassung verlangt, dass Einschränkungen von Grundrechten – hier das Recht auf informationelle Selbstbestimmung – durch ein überwiegendes öffentliches Interesse gerechtfertigt sein müssen, erscheint es als klar, dass es sich um ein Interesse des gleichen Gemeinwesens handeln muss, welches die Grundrechte einschränkt. Dies, weil nur so das angestrebte Gleichgewicht zwischen den vom Kanton gewährten Grundrechten und seinen öffentlichen Aufgaben erreicht wird. Dass andere Kantone ihre vom dortigen Gesetzgeber festgelegten Aufgaben dank des Zugriffs auf die von der Berner Verfassung geschützten Daten besser erfüllen können, kann dafür kaum ausreichen. Nur in einem überkantonalen «Rechtsraum» kann das verfassungsmässige Gleichgewicht hergestellt werden, wenn zur Erfüllung der gemeinsamen Aufgaben ein gegenseitiger Zugang zu Polizeidaten geschaffen wird. Ausserdem führen einseitige kantonale Ermächtigungen zu einem Flickwerk von Verantwortlichkeiten, technischen und organisatorischen Lösungen sowie anwendbaren Gesetzen und zuständigen Aufsichtsbehörden.

Direktionsverordnungen über die Berechtigungen der Direktionen für die zentralen Personendatensammlungen

Das im März 2021 in Kraft getretene Gesetz über die zentralen Personendatensammlungen (Personendatensammlungsgesetz, PDSG) und seine Ausführungsverordnungen (GERES V und ZPV V) erlauben eine einfache Gestaltung der Zugriffsrechte der kantonalen Behörden auf die betreffenden Datenbanken. Die Direktionen, die STA und die Justizleitung können die von ihren Organisationseinheiten benötigen Basis- und Standardprofile selbst festlegen, müssen ihre Berechtigungsregelungen aber vor dem Erlass oder einer Änderung der DSA zur formellen Stellungnahme vorlegen. Die DSA prüft, ob für die einzelnen Zugriffe eine genügende Rechtsgrundlage besteht, ob der Bedarf nach dem Zugriff im Abrufverfahren nachvollziehbar begründet ist und ob die Berechtigungen verhältnismässig ausgestaltet sind. Die Berechtigungsregelungen waren innerhalb eines Jahres nach Inkrafttreten des PDSG, d. h. bis Ende Februar 2022 zu erlassen. Im Berichtsjahr nahm die DSA zu den erstmals erlassenen und/oder geänderten Berechtigungsregelungen der BKD, der DIJ, der SID und der WEU sowie der Justizleitung Stellung. Dank des guten informellen Austausches bereits während der Erarbeitung der Regelungen konnten allfällige Differenzen so bereinigt werden, dass die DSA ihre formelle Stellungnahme kurz fassen und den Regelungen weitestgehend vorbehaltlos zustimmen konnte.

Änderung der drei Hochschulverordnungen

Zusammen mit den drei revidierten Hochschulgesetzen über die Berner Fachhochschule, die Universität und die deutschsprachige Pädagogische Hochschule traten per 1. März 2022 neue Fassungen oder Änderungen der zugehörigen Ausführungsverordnungen in Kraft. Alle drei Verordnungen sehen vor, dass die Dozierenden ihre Verwaltungsrats- und Stiftungsratsmandate offenlegen müssen und dass diese publiziert werden. An der Universität gilt die Regelung für alle Professorinnen und Professoren, an den übrigen Hochschulen nur für Dozierende mit einem «hohen» Beschäftigungsgrad. Im Mitberichtsverfahren beantragte die DSA, es sei in den Vorträgen darzulegen, aus welchen sachlichen Gründen die Unterscheidung erfolge und ab wann ein Beschäftigungsgrad als hoch gelte. Den Anliegen der DSA wurde vollumfänglich entsprochen: Während Professuren meist als Haupttätigkeit ausgeübt werden, sind die Dozierenden der anderen Hochschulen regelmässig auch in der Praxis tätig, so dass nur die Mandate von Dozierenden mit einem Beschäftigungsgrad von über 50 Prozent publiziert werden.

Verordnung über die Digitale Verwaltung

Die Verordnung über die digitale Verwaltung (DVV) ist der Ausführungserlass zum neuen DVG. Beide treten am 1. März 2023 in Kraft. Wie schon beim DVG konnte die DSA in der vorbereitenden Arbeitsgruppe zur DVV mitwirken und wichtige

Anliegen einbringen. Damit neue digitale Mittel zum Einsatz kommen können, müssen festgelegte Standards erfüllt und Prozesse eingehalten werden; bei gegebenen Voraussetzungen sind die ICT-Mittel vor dem Einsatz der DSA zur Vorabkontrolle vorzulegen. Die für den digitalen Verkehr mit Privaten notwendige Bearbeitung von Kontaktangaben wie E-Mail-Adressen, Telefon- und Mobiltelefonnummern sowie Identifikationsnummern ist in der DVV ausdrücklich geregelt. Auf die zunächst vorgesehene Verpflichtung des Kantonspersonals, private Mobiltelefone für dienstliche Zwecke einsetzen zu müssen, wurde angesichts einer fehlenden Grundlage im DVG verzichtet. Aus Datenschutzsicht wäre es vertretbar gewesen, diejenigen Mitarbeitenden zur Bekanntgabe der privaten Mobiltelefonnummer zu verpflichten, welche einen Gerätebeitrag und/oder ein kostenloses oder vergünstigtes Abonnement erhalten. Die Grundsätze und Anforderungen für den elektronischen Behördenverkehr in Verwaltungsverfahren werden im Gesetz über die Verwaltungsrechtspflege geregelt werden.

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 134 Vorabkontrollen und Vorprüfungen (Vorjahr: 138) zu Informatikprojekten bearbeitet und dabei 94 (77) bzw. 68 % (55.8) der Geschäfte abgeschlossen. Diese 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.

ERP-System Kanton Bern

Mit dem neuen Enterprise Resource Planning (ERP)-System des Kantons Bern wurden in einer ersten grossen Etappe per 1. Januar 2023 die alten Finanz- und Personalinformationssysteme FIS und PERSISKA abgelöst. Die DSA prüfte die ISDS-Dokumentation für das neue ERP-System in mehreren Vorabkontrollschritten umfassend. Ergänzend prüfte sie die Lösung PANSYS, die dem Personalamt für eine Übergangsphase als Archivsystem für bestimmte Teile von PERSISKA dient. Im ERP-System war bzw. ist auf Verlangen der DSA eine wichtige Anpassung bei den Berechtigungen vorzunehmen: Aktuell können Mitarbeitende des Finanzbereichs auch Daten anderer Ämter der gleichen Direktion einsehen, obwohl sie diese für die Aufgabenerfüllung nicht benötigen. Damit besteht ein hohes Risiko, das Datenschutzrecht sowie gegebenenfalls Amtsgeheimnisse und besondere Geheimhaltungspflichten zu verletzen. Die Projektverantwortlichen bestätigten der DSA, dass die Berechtigungen baldmöglichst technisch eingeschränkt werden. Bis dahin erliessen die Direktionen eine Weisung an die betroffenen Mitarbeitenden, wonach es diesen untersagt ist, auf für die Aufgabenerfüllung nicht benötigte Daten zuzugreifen. Die Zugriffe im ERP-System werden geloggt und mittels Stichproben auf ihre Rechtmässigkeit überprüft.

Zentrales Scanning der Kreditoren-Rechnungen der Kantonsverwaltung sowie der Posteingänge der Betreibungs- und Konkursämter

Das KAIO unterbreitete der DSA den Service Inputmanagement Kreditoren-Rechnungen der Swiss Post Solutions (SPS) AG zur Vorabkontrolle. In Zukunft werden alle eingehenden Kreditoren-Rechnungen, Gutschriften und Mahnungen im Kanton Bern an einer zentralen Stelle digital erfasst und bearbeitet. Der Service umfasst auch die Anbindung der Scanning-Plattform der Leistungserbringerin an das Kreditorenworkflow-System des ERP Kanton Bern (SAP VIM). Die SPS AG gehörte der Schweizerischen Post und wurde im Laufe des Jahres 2022 integral an die AS Equity Partners GmbH verkauft und übergeben. Die Empfehlungen der DSA betrafen namentlich die Aspekte, dass die temporär zwischengespeicherten Daten verschlüsselt werden und dass private, vertrauliche und geheime Sendungen von der Leistungserbringerin nicht verarbeitet, sondern ungeöffnet an die Empfängerin oder den Empfänger weitergeleitet werden. Eine Verletzung der Vorgaben ist mit einer Konventionalstrafe bewehrt.

Mit den gleichen technischen und organisatorischen Grundleistungen sollen im Rahmen des Projekts «Digipost@DIJ-BAKA» schrittweise auch die Posteingänge der Betreibungs- und Konkursämter zentral gescannt sowie die digitalisierten Dokumente an deren Fachapplikationen übergeben werden. Die betreffenden ISDS-Unterlagen basierten darum weitgehend auf jenen für das Inputmanagement Kreditoren-Rechnungen, und die DSA konnte in der Vorabkontrolle ebenfalls auf die dortigen Feststellungen zurückgreifen.

Beide Vorabkontrollen gelangten zum Ergebnis, dass die Prozesse datenschutzkonform erfolgen können, dass aber vor der Überführung des Betriebs vom Rechenzentrum der Post in jenes der Swisscom (infolge der Übernahme der SPS AG) darzulegen sein wird, dass der Datenschutz und die Informationssicherheit auch beim neuen Leistungserbringer gewährleistet sind.

BE-GEVER Mandantenkopien

Das KAIO unterbreitete der DSA eine Ergänzung des ISDS-Konzepts für die elektronische Geschäftsverwaltung (BE-GEVER) der Kantonsverwaltung, wonach alle Daten in allen Mandaten der Direktionen und Ämter wiederkehrend vom produktiven in das Testsystem kopiert werden sollten, um dort für Tests und Schulungen zur Verfügung zu stehen. Die DSA erachtete weder die Rechtmässigkeit noch die Verhältnismässigkeit als dargelegt: Die Bearbeitung von Personendaten zu Test- oder Schulungszwecken dient einem anderen Zweck als jenem, für den die Daten ursprünglich beschafft wurden. Wegen des Grundsatzes der Zweckbindung (Art. 5 Abs. 4 KDSG) muss deshalb für den neuen Bearbeitungszweck eine genügende Rechtsgrundlage bestehen, welche entweder die Datenbearbeitung selbst oder eine Aufgabe regelt, zu deren Erfüllung die Datenbearbeitung notwendig ist. Wird der ordnungsgemässe Betrieb und Unterhalt von BE-GEVER als gesetzliche Aufgabe der Kantonsverwaltung angesehen, so ist immer noch darzulegen, warum Tests mit echten Personendaten notwendig sind und es nicht möglich ist, mit fiktiven Daten zu arbeiten. Der blosse Aufwand für die Erstellung von geeigneten Testfällen kann jedenfalls keine Rechtfertigung für Grundrechtseingriffe durch eine Zweckentfremdung von Personendaten sein. In Ausnahmefällen können Tests mit echten Daten zwingend erforderlich sein, namentlich um eine Schnittstelle zu einem System zu testen, welches über keine Testumgebung verfügt. Auch dann muss der Umfang der verwendeten Daten verhältnismässig – d. h. auf die notwendige Zahl beschränkt – sein, was bei der geplanten Vollspiegelung nicht der Fall gewesen wäre.

Die Beurteilung der DSA änderte sich, als das Vorhaben auf Wunsch des Staatsarchivs (StAB) auf eine einmalige Kopie von vier ausgewählten Mandanten beschränkt wurde. Damit sollte es ermöglicht werden, im Rahmen eines Projekts die Funktionalitäten, Performance, Durchlaufzeit und praktische Umsetzbarkeit der elektronischen Ablieferung der archivwürdigen Daten an das StAB zu testen und die Daten im Testsystem anschliessend wieder zu vernichten. Hier konnte die DSA die zwingende Notwendigkeit der Tests mit echten Daten nachvollziehen: Der Ablieferungsprozess ist irreversibel und muss daher im Vorfeld realitätsnah getestet werden, damit nicht erst bei der produktiven Einführung schwerwiegende Fehler auftreten, die nicht mehr korrigiert werden können und einen unwiederbringlichen Datenverlust zur Folge hätten. Eigens erstellte Testdaten können die Heterogenität und das Mengengerüst der Produktivdaten nicht hinreichend nachbilden. Durch die Beschränkung auf vier Mandanten und die Dauer des Projekts erachtete die DSA auch die Verhältnismässigkeit als gegeben.

Fachapplikation «AssistMe»

Das kantonale Behindertenkonzept will die Eigenverantwortung und die soziale Teilhabe von erwachsenen Menschen mit Behinderungen stärken und garantiert deshalb die freie Wahl zwischen dem Leistungsbezug in Institutionen (Wohnheime, Tages- und Werkstätten) und dem ambulanten Leistungsbezug (Assistenz, Coaching am Arbeitsplatz). Jede Person hat hierbei Anspruch auf diejenigen Leistungen, welche zur Deckung des individuellen, behinderungsbedingten Betreuungs- und Pflegebedarfs erforderlich sind. In der Praxis heisst das, dass die betroffenen Menschen direkt mit dem Kanton abrechnen bzw. die Kostenbeteiligung einfordern. Dazu müssen sie ihre behinderungsbedingten Ausgaben sowie die finanziellen Beiträge aller Leistungsfinanzierenden (Sozialversicherungen, Krankenkassen) in einem Abrechnungssystem erfassen. Diese Abrechnung wird vom Kanton überprüft und der korrekte Nettobetrag ausbezahlt. Für die Umsetzung des Systemwechsels wird deshalb aktuell eine webbasierte Lösung entwickelt, die das bisher auf Excel basierende Abrechnungssystem für Menschen mit Behinderungen im Kanton Bern ablöst.

In diesem Zusammenhang stellte das Amt für Integration und Soziales (AIS) der DSA die angepasste ISDS-Dokumentation für die Applikation «AssistMe» zur Prüfung zu. Die Applikation – früher mit der Bezeichnung «IBAS» – war 2019 von der DSA vorabkontrolliert worden, befindet sich heute in einem produktiven Pilotbetrieb und soll im Hinblick auf die Inkraftsetzung des Behindertenleistungsgesetzes per 01.01.2024 erweitert und angepasst werden. Nachdem das ISDS-Konzept auf Empfehlung der DSA in wichtigen Punkten – namentlich zum Testkonzept, zur Datenmigration, zur sicheren Authentifizierung der Benutzenden und zur Anbindung an das neue ERP-System – ergänzt wurden, konnte die Vorabkontrolle erfolgreich abgeschlossen werden.

Ausserbetriebnahme der Fachapplikation SORMAS

Für das Covid-19 Kontaktmanagement verwendete die GSI die Fachapplikationen SORMAS (Surveillance and Out-break Response Management System) und TRACY. Mit diesen Applikationen bearbeitete die GSI personenbezogene Gesundheitsdaten und damit besonders schützenwerte Personendaten. Die Applikationen unterlagen deshalb der Vorabkontrolle durch die DSA. Im Hinblick auf die Einstellung des Kontaktmanagements per April 2022 schloss die DSA im März die Vorabkontrolle ab, obwohl ihr bis zu diesem Zeitpunkt nie vollständige ISDS-Unterlagen vorlagen. Stattdessen prüfte sie in einem separaten Verfahren die Ausserbetriebnahme von SORMAS, insbesondere die vollständige Löschung bzw. Anonymisierung der damit bearbeiteten Gesundheitsdaten. Diese Prüfung konnte die DSA nach drei formellen Schriftenwechseln erfolgreich abschliessen.

Fachapplikation «Minddistrict»

Die Privatklinik Wyss AG ist bestrebt, die Integration von Online-Interventionen in die reguläre Psychotherapie (sog. «Blended Treatment») als Ergänzung zur herkömmlichen Therapie in ihrem Behandlungsangebot zu etablieren. Die Klinik plante deshalb die Einführung des webbasierten Standardprodukts «Minddistrict E-Mental-Health-Plattform» («Minddistrict»), einer Plattform zur psychischen Gesundheitsvorsorge. Sie trat frühzeitig an die DSA heran, um mit ihr die Durchführung der Vorabkontrolle zu planen und die Applikation mit Blick auf die besonders schützenswerten Personendaten auf die Datenschutzkonformität hin zu überprüfen.

Konkret unterstützt die Applikation «Minddistrict» den persönlichen Genesungsweg eines Menschen von der Prävention bis zur Nachsorge mit diversen Angeboten und Funktionen. Daneben ermöglicht «Minddistrict» insbesondere evidenzbasierte Online-Interventionen und zertifizierte Videosprechstunden, wobei Letztere von der Klinik nicht genützt werden. Für die Patientinnen und Patienten besteht bei «Minddistrict» ausserdem die Möglichkeit, ein Tagebuch zu führen. Behandlungsdokumentationen werden jedoch nicht in «Minddistrict» geführt, sondern ausschliesslich im Klinikinformationssystem der Privatklinik Wyss. Ein wesentlicher Befund der DSA betraf die aus ihrer Sicht zu lange Aufbewahrungsdauer von 15 Jahren. In ihrer Stellungnahme wies die Klinik darauf hin, dass es oft zu Rückfällen komme, die zu einem Wiedereintritt in die Klinik führten; dabei sei die Möglichkeit einer Wiederaufnahme des letzten Therapiestandes sehr wertvoll. Sobald ein Konto deaktiviert werde – was drei Monate nach dem Austritt erfolge – habe niemand mehr Zugriff auf die Daten. Damit erachtete die DSA die Aufbewahrungsfrist als fachlich begründet.

Klinikinformationssystem «EPIC KISS»

Die von der Insel Gruppe AG neu eingeführte Applikation EPIC – welche den Namen des amerikanischen Systemanbieters trägt – wird als neues Klinikinformationssystem erstmals zusätzlich mit einer Steuerungsfunktion verbunden sein (deshalb KISS). Die Applikation soll die berufs- und fachübergreifende Behandlung der Patientinnen und Patienten ermöglichen und für jede betroffene Person alle Gesundheitsinformationen in einem einzigen Dossier überall und jederzeit bereitstellen. Zudem sollen in EPIC KISS durch die strukturierte und durchgängige Erfassung der Daten deren Auswertung möglich werden sowie die Behandlungsqualität und Sicherheitsstandards im Behandlungsprozess gewährleistet sein.

Als die DSA von der geplanten Einführung von EPIC KISS erfuhr, insistierte sie gegenüber der Insel Gruppe auf ihre Involvierung. Die Insel Gruppe begrüsste die Begleitung des Projekts durch die DSA bereits im Zeitpunkt vor der Erarbeitung der ISDS-Unterlagen. Wegen des Wechsels von einer

fallgesteuerten zu einer patientengesteuerten Behandlungsdokumentation über die Institutionen der Insel Gruppe ist davon auszugehen, dass sich die klare Trennung der Einsicht in einzelne medizinische Behandlungen aufweichen wird. Die DSA kommunizierte der Insel Gruppe deshalb von Beginn an, dass das insoweit offenere System ausreichende Massnahmen vorsehen muss, damit das Verhältnismässigkeitsprinzip beim Zugang zu Personendaten gewahrt bleibt. Bevor die Insel Gruppe die ISDS-Dokumentation zur Vorabkontrolle einreichen wird (voraussichtlich im Jahr 2023), soll eine Demonstration stattfinden, welche eine erste Beurteilung der Applikation hinsichtlich der vorgesehenen Zugriffsregelungen erlauben wird. Die Ausgestaltung der Zugriffssteuerung wird aufgrund der Abhängigkeit der Systeme auch für die Fachapplikation «Medical Content Plattform» – das Health Content Management System – relevant sein. Diese Lösung soll den medizinischen Fachpersonen einen Grossteil der medizinischen Inhalte zur Verfügung stellen. Darunter sind konkret alle Medien in Form von Bildern, Dokumenten, Biosignalen, Videos und Audiodateien zu verstehen, welche in Expertensystemen produziert oder von externen Zuweisende oder Partnerinstitutionen zur Verfügung gestellt werden.

Fachapplikation «eArchiv ARTS»

In den Universitären Psychiatrischen Diensten Bern (UPD) wurden die Behandlungsdokumentationen bis anhin papierbasiert und/oder digital aufbewahrt. Für die Einführung der Applikation «eArchiv ARTS» kontaktierten die UPD die DSA frühzeitig für die Durchführung der Vorabkontrolle, um die Datenschutzkonformität zu gewährleisten. Bei «eArchiv ARTS» handelt es sich um ein dokumentenbasiertes digitales Universalarchiv zur ordnungsgemässen und gesetzeskonformen Aufbewahrung von Daten und Dokumenten der Patientinnen und Patienten. Die Feststellungen und Empfehlungen der DSA waren vorwiegend technischer Art und darauf ausgerichtet, die Informationssicherheit der Daten zu gewährleisten. Gestützt auf die Erklärungen bzw. Ergänzungen der ISDS-Unterlagen durch die UPD konnte die Vorabkontrolle ohne wesentliche Befunde 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 Rückspracheverfahren 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.

Neben dem PolG enthält seit Ende 2018 auch das Justizvollzugsgesetz (JVG) Vorschriften über die Videoüberwachung in Vollzugseinrichtungen und Transportfahrzeugen, welche zur Aufgabenerfüllung – namentlich zur Gewährleistung der Sicherheit und Ordnung sowie zum Schutz des Personals, der Eingewiesenen und Dritten an den betreffenden Orten – eingesetzt werden dürfen. 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).

Rückkehrzentren Aarwangen und Gampelen

Das Amt für Bevölkerungsdienste (ABEV) ist für die Gewährung der Nothilfe für abgewiesene Asylsuchende zuständig und betreibt namentlich in Aarwangen und Gampelen je ein Rückkehrzentrum. Mit deren Führung hat das ABEV die Firma ORS Service AG (ORS) beauftragt.

Im Zentrum Aarwangen lebten im Zeitpunkt der Vorabkontrolle vor allem Familien mit schulpflichtigen Kindern. Zu deren Schutz vor sog. «Fremdschläfern» – d. h. nicht zutrittsberechtigten Drittpersonen – und um bei Eskalationen unter den Bewohnerinnen und Bewohnern zeitnah eingreifen zu können, plante das ABEV eine Echtzeitüberwachung der Hintereingänge und der Erschliessungsgänge zu den Zimmern bzw. Wohnungen während der Nacht sowie an Wochenenden und Feiertagen, wenn weniger Personal der ORS vor Ort anwesend ist. Im Rahmen der Vorabkontrolle beurteilte die DSA die zeitlich beschränkte Überwachung ohne Aufzeichnung als verhältnismässig.

Das Zentrum Gampelen ist auf einem weitläufigen Gelände mit teils schlecht einsehbaren Nebengebäuden bzw. Eingängen gelegen, der Zugang zum Gelände kann weder baulich eingeschränkt noch vollständig kontrolliert werden. Die Bewohner waren fast ausschliesslich erwachsene Personen, grossmehrheitlich junge Männer, wovon einige mit schweren psychischen Auffälligkeiten. Deren Perspektivenlosigkeit in Verbindung mit Alkohol- und Drogenkonsum/-handel führte laut ABEV zu einem deutlich höheren Risiko von physischer Gewalt – auch durch nicht zutrittsberechtigte Dritte – gegen das Personal und Mitbewohnende sowie anderen Straftaten. Auch in Gampelen sollte einerseits mittels (hier ganztägiger) Echtzeitüberwachung die Interventionszeit verkürzt werden; andererseits sollte auch eine Aufzeichnung erfolgen, um bei einer Straftat das Bildmaterial als Beweismittel an die KAPO aushändigen zu können. Gegen das Argument des ABEV, ohne Videoüberwachung wäre mehr teures Sicherheitspersonal erforderlich, wandte die DSA ein, dass sich Grundrechtseingriffe nicht allein mit einer Kostenoptimierung rechtfertigen lassen. Sie verlangte deshalb einerseits Angaben zum Personalbestand vor Ort und anderseits eine Zusammenstellung der Vorfälle in den letzten zwei Jahren, in denen eine Echtzeitüberwachung bzw. Aufzeichnung wichtig gewesen wäre. Auf dieser Grundlage und unter Berücksichtigung der

eingangs geschilderten Umstände sowie der grossen Distanz zum nächsten Polizeiposten hielt die DSA die Videoüberwachung für verhältnismässig. Gleichzeitig behielt sie sich vor, die weitere Entwicklung der Vorfälle zu beobachten, um die Wirksamkeit und Verhältnismässigkeit der Massnahmen bei Bedarf neu zu beurteilen.

Im Mitberichtsverfahren zur Antwort des Regierungsrates auf die Interpellation 103-2022 Junker Bernhard («Videoüberwachung in Rückkehrzentren») erwirkte die DSA, dass ihre Anforderung betreffend die Dokumentation und weitere Beobachtung der Anzahl videorelevanter Vorfälle in die Antwort an den Grossen Rat aufgenommen wurde.

Gefängnisse und Justizvollzugsanstalten

Im Jahr 2010 hatte die DSA in sehr pauschaler Weise die Videoüberwachungen in allen Gefängnissen und Justizvollzugsanstalten des Kantons Bern vorabkontrolliert. Seither traten die Vorschriften des JVG in Kraft und die Überwachungssysteme der Einrichtungen wurden im Zuge des technischen Fortschritts teilweise umfassend erneuert und ausgebaut.

Vor diesem Hintergrund nahm das Amt für Justizvollzug (AJV) in Absprache mit der DSA ab 2020 die vollständige Erneuerung der ISDS-Unterlagen pro Einrichtung an die Hand. Im Rahmen von Besichtigungen im Regionalgefängnis Thun, in der Justizvollzugsanstalt Hindelbank und im Massnahmenzentrum St. Johannsen konnte sich die DSA einerseits ein Bild von den Verhältnissen und Bedürfnissen machen und anderseits die Anforderungen an eine rechtskonforme Videoüberwachung erläutern. Auf dieser Grundlage beurteilte die DSA im Berichtsjahr die ISDS-Unterlagen für die Regionalgefängnisse Bern, Biel, Burgdorf und Thun, die Justizvollzugsanstalt Hindelbank, das Massnahmenzentrum St. Johannsen, das Regionalgericht Bern-Mittelland (Provisorium im Amtshaus), die Bewachungsstation im Inselspital und den Transportdienst des AJV. Ihre Empfehlungen pro Einrichtung – zu denen namentlich die Verpixelung des Sanitärbereichs in Sicherheitszellen und des öffentlichen Raums ausserhalb der Einrichtungen gehörte – wurden vom AJV angenommen und umgesetzt, womit die DSA die Datenschutzkonformität der heutigen Videoüberwachungen (präzis: der dafür erstellten Konzepte) bestätigen konnte.

Videoüberwachung am Inselspital

Für das Inselspital waren zwei Videoüberwachungsanlagen zu beurteilen: eine für das Wartezimmer der Hämatologie und eine für die Stationen D und E der Kinderklinik. In beiden Fällen handelte es sich um Echtzeitüberwachungen der Patientinnen und Patienten aus medizinischen Schutzgründen, also nicht für polizeiliche Zwecke und damit nicht nach den Vorschriften des PolG.

Dabei stellte sich die Frage, inwieweit die Videobilder bei der Übertragung innerhalb der von der Insel Gruppe AG als sicher beurteilten Netzsegmente zusätzlich verschlüsselt werden sollten (in öffentlichen Netzen ist eine Transportverschlüsselung absolut erforderlich). Die DSA empfahl, eine zusätzliche Verschlüsselung mittelfristig vorzusehen und wird bei der Prüfung der gesamten technischen Video-Grundinfrastrukturanlage darauf zurückkommen.

6.4 Audits

Die DSA führte im Rahmen ihres gesetzlichen Auftrags, die Anwendung der Vorschriften über den Datenschutz und die Informationssicherheit zu überwachen, insgesamt 12 ISDS-Audits durch, wovon vier in Zusammenarbeit mit der FK. Das geplante ISDS-Audit des Kerninformatiksystems «Rialto» der KAPO wurde aufgrund der für 2023 vorgesehenen Sonderprüfung durch die FK zurückgestellt. Die Zusammenarbeit mit der FK wird im Jahr 2023 weitergeführt.

Entsprechend ihrer für die Jahre 2019–2023 formulierten Strategie fokussierte sich die DSA bei der Prüfung risikoorientiert auf Kernfachanwendungen und ICT-Grundversorgungsservices sowie auf die Gesundheitsbranche. Weiter begleitete die DSA kontinuierlich die Umsetzung von Verbesserungsmassnahmen der in den Vorjahren durchgeführten ISDS-Audits. Dabei konnte u. a. die Einführung von Zugriffskontrollmassnahmen im Geschäftsverwaltungssystem der Kindes- und Erwachsenenschutzbehörden erfolgreich abgeschlossen werden.

Die Begleitung der Umsetzung von Massnahmen stellt eine sehr wirksame und zielführende Standardaufgabe der DSA dar. Dazu gehören auch dezidierte Nachprüfungen, um sicherzustellen, dass die festgestellten Mängel von den verantwortlichen Stellen tatsächlich und damit nachweisbar behoben wurden. Die DSA musste in den vergangenen Jahren wiederholt feststellen, dass die ISDS-Aufgaben zu wenig Aufmerksamkeit von den verantwortlichen Stellen erhielten. Auch im 2022 konnte diese notwendige Aufmerksamkeit teils noch nicht im gewünschten Masse festgestellt werden. ISDS-Aufgaben wurden oft «nebenbei» wahrgenommen. Fehlende Aufmerksamkeit und damit die verzögerte Umsetzung von ISDS-Verbesserungsmassnahmen erhöhen jedoch das Risiko, dass auf die generelle Bedrohungslage – die kriminellen Cyberaktivitäten bewegten sich auch im Berichtsjahr auf hohem Niveau – nicht zeitnah reagiert werden kann. Die Zeitspanne zwischen dem Erkennen eines Mangels bis zur effektiven Behebung ist vielfach zu gross. Auch muss die Widerstandsfähigkeit gegenüber Cyberrisiken von den verantwortlichen Stellen periodisch überprüft und bei Bedarf durch geeignete Massnahmen angepasst werden. Sodann musste festgestellt werden, dass bei der nachweisbaren Einhaltung rechtlicher

Vorgaben teilweise noch erheblicher Verbesserungsbedarf besteht. Erfreulich im Berichtsjahr war indes, dass Verantwortungsträger vermehrt den Kontakt zur DSA suchten, um ihre aktuelle Situation zu erläutern und im Dialog Verbesserungsmassnahmen aufzuzeigen.

Selbstdeklaration Klinik Bethesda

Die Klinik Bethesda ist auf die Behandlung von Menschen mit neurologischen Erkrankungen spezialisiert und bezeichnet sich als eine der führenden Spezialkliniken für neurologische Rehabilitation. Medizinische Behandlung, Pflege und Therapien sind Schwerpunkte der Patientenbetreuung. Die Klinik Bethesda beschäftigt über 300 Mitarbeitende.

Im Fokus der Prüfung stand die Beurteilung der ISDS-Selbstdeklaration der Klinik. Die von der DSA dafür zur Verfügung gestellten Hilfsmittel umfassten drei Checklisten, welche die wesentlichen ISO/IEC 27001/2 ISDS-Controls (massgebende ISDS-Aufgaben pro Themenfeld) zu der ICT-Organisation der Klinik Bethesda, den externen ICT-Dienstleistern (mit Sicht auf einen ICT-Kerndienstleister) und der Kernfachanwendung abbildeten. Die Beurteilung der DSA erfolgte primär mit Sicht auf ISDS-Risiken sowie sekundär auf Vollständigkeit, Nachvollziehbarkeit und Prüfbarkeit der selbstdeklarierten Ausgangslage.

Die DSA hat zusammenfassend den Eindruck erhalten, dass bei der Klinik Bethesda betreffend Datenschutz und Informationssicherheit bereits ein annehmbarer Stand erreicht worden ist. Grundsätzlich ist eine der Organisationsgrösse und Datenbearbeitung angemessene Aufmerksamkeit für die ISDS-Aufgaben vorhanden. Dennoch besteht ein erkennbarer Verbesserungs- und Optimierungsbedarf. Dieser wurde mit einer mittleren, aber zum Teil auch hohen Wesentlichkeit eingestuft. Die Klinik Bethesda hat die bestehenden Defizite erkannt und wird Verbesserungsmassnahmen planen und umsetzen. Die DSA wird in der Folge den Fortschritt und die Ergebnisse überprüfen. Die Zusammenarbeit erfolgte in einem stets freundlichen und professionellen Umfeld.

Grundschutz Privatklinik Wyss AG

Die Privatklinik Wyss bietet ihre ambulanten, tagesklinischen und stationären Leistungen seit 1845 für Patientinnen und Patienten mit psychischen Erkrankungen an. Sie beschäftigt am Hauptstandort in Münchenbuchsee und an den weiteren Standorten in Bern und Biel zusammen rund 340 Mitarbeitende.

Die Prüfungshandlungen fokussierten sich auf die ISDS-Anforderungen und wie diese durch den ICT-Grundschutz erfüllt werden. Der Grundschutz umfasst alle Verfahren, Massnahmen, Organisation, Prozesse, Hilfsmittel, Infrastruktur und

technische Systeme, Daten und Vorkehrungen etc., welche die sichere und datenschutzkonforme Abwicklung der Geschäftsprozesse einschliesslich der Datenbearbeitungen bei der Privatklinik Wyss AG unterstützen.

Im Rahmen der Prüfung wurden über alle Prüfbereiche hinweg Befunde festgehalten. Der überwiegende Teil der Prüfbereiche umfasste Befunde, die mit einem höheren Risiko eingestuft wurden. Insgesamt konnte aber auch festgehalten werden, dass bei der Privatklinik Wyss bereits grundlegende und zielführende Massnahmen ergriffen wurden, um die Informationssicherheit und den Datenschutz zu verbessern. Die DSA wird die Umsetzung von Empfehlungen aktiv begleiten. Die Prüfung erfolgte in einem freundlichen und kooperativen Umfeld.

Grundschutz Spital Langenthal (SRO AG)

Die SRO AG ist das regionale Spitalzentrum im Oberaargau. Neben dem Spital Langenthal betreibt sie Gesundheitszentren und Wohneinrichtungen. Die SRO AG beschäftigt ca. 1 100 Mitarbeitende.

Die DSA hatte im 2019 bei der SRO AG eine Prüfung des ICT-Grundschutzes durchgeführt. Das Gesamtergebnis der Prüfung wies zu diesem Zeitpunkt in allen Prüfbereichen ein deutliches Verbesserungs- und Optimierungspotential aus. Insgesamt wurden damals 28 Befunde mit Empfehlungen festgehalten. Im Jahr 2022 führte die DSA eine Nachrevision durch. Diese Prüfung umfasste das Beurteilen der Umsetzung von Empfehlungen und den nachweisbaren Betrieb von ISDS-Massnahmen.

Bei der Nachrevision konnten zehn Empfehlungen als umgesetzt betrachtet werden. Bei 13 Empfehlungen wurde die Situation als teilweise, aber noch nicht vollständig umgesetzt beurteilt. Bei fünf Empfehlung ist die Umsetzung noch ausstehend. Die DSA wird die Umsetzung der noch verbleibenden Verbesserungsmassnahmen weiterhin aufmerksam begleiten. Die Nachrevision erfolgte in einem professionellen und konstruktiven Umfeld.

Grundschutz Regionalspital Emmental AG

Das Regionalspital Emmental AG erbringt medizinische Dienstleistungen und unterhält die zwei Standorte Burgdorf und Langnau. Das Dienstleistungsangebot umfasst die Grundversorgung in den Hauptdisziplinen Chirurgie, Medizin sowie Gynäkologie und Geburtshilfe, erweitert durch ein Angebot von Spezialdisziplinen. Das Spital verfügt über ca. 950 Vollzeitstellen ohne Auszubildende. Im Jahr 2021 wurden ca. 10 500 Fälle behandelt. Das Spital verfügt über eine interne ICT-Organisation, welche die massgebenden ICT-Dienstleistungen zur Verfügung stellt. Mit der Prüfung wurde der ICT-Grundschutz in Bezug auf die einschlägigen Normen und Rahmenwerke wie ISO/IEC 27001, 27701 bzw. Grundschutz

gemäss dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) und die nachweisbar implementierten Massnahmen (Prozesse, Aufgaben, Kontrollen, Infrastruktur, Organisation) zur Erfüllung von ISDS-Anforderungen beurteilt. Dabei wurden die Prüfgebiete ICT-Governance, ISDS-Konzepte, Change- und Release-Management, Zugriffs-Management, Netzwerksicherheit, Client- und Serversicherheit, Outsourcing und die physische Sicherheit (der Rechenzentren) berücksichtigt.

Zum Zeitpunkt der Erstellung des vorliegenden Berichts lag das konsolidierte Ergebnis der Prüfung noch nicht vor. Die Prüfung erfolgte in einem durchwegs guten Einvernehmen und freundlichen Umfeld.

Endgeräte Kantonspolizei Bern

Die KAPO sorgt mit geeigneten Massnahmen, Information und Beratung für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung. Das Korps der KAPO umfasst rund 2 700 Mitarbeitende und wird vom Kommandanten geleitet. Die KAPO verfügt über eine interne Informatikorganisation, welche in Zusammenarbeit mit externen Dienstleistern ICT-Services zur Verfügung stellt.

Die durchgeführte Prüfung umfasste ein mehrteiliges technisches Security-Audit der KAPO-Endgeräte, auch Clients genannt. Im Fokus stand der KAPO Standard-Client mit dem Windows 10 Betriebssystem. Dabei wurde die Konfiguration des Clients grundsätzlich auf die Umsetzung von Security-Best-Practices hin überprüft. Darüber hinaus wurde das ISDS-Konzept für Windows-Clients und -Infrastruktur in die Prüfung miteinbezogen. Dies hatte zum Ziel, die darin festgehaltenen Risiken und Massnahmen (Soll) mit dem tatsächlichen Zustand (Ist) des zur Verfügung gestellten Standard-Clients abzugleichen und sicherheitsrelevante Punkte kritisch zu hinterfragen. Zudem erfolgte eine Analyse des Netzwerkverkehrs des Clients. Weiter wurden sowohl ein FAT-Client (physischer Client) als auch ein VDI-Desktop (virtueller Client) einem Penetrationstest unterzogen. Vordergründiges Ziel des Tests war es aufzuzeigen, ob Schwachstellen zur Ausweitung der Berechtigungen identifiziert und ausgenutzt werden konnten.

Die Resultate des Penetrationstests stellten der untersuchten Umgebung ein mittelmässiges Zeugnis aus. Die Umgebung war nicht nach aktuellen Best Practices konfiguriert und wies eine Vielzahl von unsicheren Konfigurationen und Sicherheitslücken auf. Zudem wurden beim Windows FAT-Client eine Vielzahl an Sicherheitsrisiken identifiziert. Einige wurden als «hoch» eingestuft. Massnahmen zur Behebung der festgestellten Mängel wurden von der KAPO umgehend geplant und angegangen. Die DSA wird die Umsetzung der Verbesserungsmassnahmen aufmerksam begleiten. Die Prüfung erfolgte in einem professionellen und freundlichen Umfeld.

Fachanwendung «NFAM»

Die neue Fachanwendung Migration NFAM stellt Funktionen für die einheitliche, durchgehende und direktionsübergreifende Fall- und Dossierführung im Bereich der Integration und für alle weiteren ausländerrechtlichen Prozessen des Kantons zur Verfügung. Dabei ist die GSI für alle Belange der Asyl- und Flüchtlingssozialhilfe zuständig. Regionale Partner übernehmen die Verantwortung für die operative Umsetzung. Innerhalb der GSI ist das AIS für die Sozialhilfe, die Arbeitsintegration von Behinderten und Flüchtlingen/Asylbewerbern sowie für Kinder-/Jugendarbeit und Kindertagesstätten zuständig. Es trägt die Gesamtverantwortung für den Asylprozess. Die SID bzw. der Migrationsdienst des ABEV erfüllt alle Aufgaben rund um Einreise, Aufenthalt und Arbeit von Ausländerinnen und Ausländern im Kanton Bern, die in seine Zuständigkeit fallen.

Die Prüfungshandlungen betrafen schwergewichtig die ISDS-Umsetzung und den Betrieb unter Einbezug der ISDS-Governance, ISDS-Konzeption, Berechtigungsmanagement, Datenhaltung und Schnittstellen sowie der externen Dienstleistungen und des Outsourcings.

Es wurden über alle Prüfbereiche hinweg Befunde festgehalten. So wurden von der DSA in der Vorabkontrolle (Art. 17a KDSG) empfohlene Massnahmen nicht nachvollziehbar umgesetzt. Weiter waren die strategische ISDS-Lenkung und die operative ISDS-Steuerung zu wenig erkennbar. Regulatorisch vorgegebene ISDS-Kontrollaufgaben wurden nicht genügend wahrgenommen. Die ISDS-Dokumentation (ISDS-Konzept) und die Risikoanalyse waren nicht aktuell, und bei der Softwareprogrammierung wurden den ISDS-Prinzipien «Security by Design» und «Privacy by Default» zu wenig Beachtung geschenkt. Beim Berechtigungsmanagement zeigte sich Optimierungsbedarf. Auch musste festgestellt werden, dass die Datenbearbeitung in den Testsystemen mit produktiven Daten erfolgte. Die erkannten Mängel und die daraus folgenden Risiken stufte die DSA als wesentlich ein. Die Prüfung wurde in enger Zusammenarbeit mit der FK durchgeführt und gestaltete sich u. a. aufgrund der komplexen Ausgangslage als schwierig.

Fachanwendung «NESKO»

Der Kanton Bern verbucht jährlich ca. 6 Milliarden Franken an Steuereinnahmen, wobei die Steuerdaten mit dem ICT-System NESKO der SV verarbeitet werden. Die für die Veranlagung der natürlichen Personen eingesetzte Fachanwendung NESKO VA-NP ist eines der grundlegendsten ICT-Systeme der SV. Sie ist bereits langjährig in Betrieb und gilt als robust. Die ISDS-Konformität der Fachanwendung ist von hoher Bedeutung, entsprechend ist der ISDS-Analyse sowie der Konzeption um Umsetzung von wirkungsvollen ISDS-Massnahmen sehr grosses Gewicht beizumessen, um Risiken wie unbefugten Zugriffen oder Datenverlust angemessen begegnen zu können.

Die Prüfungshandlungen konzentrierten sich unter Einbezug der ISDS-Governance auf die ISDS-Umsetzung und den ISDS-Betrieb, die ISDS-Konzeption, das Berechtigungsmanagement, die Datenhaltung und die Schnittstellen sowie die externen Dienstleistungen und das Outsourcing.

Bei der Prüfung wurde u. a. festgestellt, dass es Lücken in der ISDS-Governance gibt. So fehlt eine stringente ISDS-Strategie und die Zuständigkeiten (Dateneigner) sind nicht zielführend festgelegt. Die Schlüsselrolle «Sicherheitsverantwortliche» verfügt über ungenügende Ressourcen für die zugeordneten Aufgaben. Weiter sollten für die Fachanwendung VA-NP und für weitere relevante NESKO-Fachanwendungen je aktuelle ISDS-Konzepte erstellt sowie das unzureichende Management der Zugriffsberechtigungen gelöst werden. Bei der Softwareentwicklung besteht mit Blick auf die nachweisbare Berücksichtigung der ISDS-Prinzipien «Security by Design» sowie «Privacy by Default» erkennbar Optimierungsbedarf. Die Prüfung erfolgte in enger Zusammenarbeit mit der FK und insgesamt in einem professionellen Umfeld mit gutem Einvernehmen.

Fachanwendung «GELAN»

Die Gesamtlösung EDV Landwirtschaft & Natur (GELAN) steht in den Kantonen Bern, Fribourg und Solothurn im Einsatz. Das Agrarinformationssystem wurde laufend weiterentwickelt und auf 15 vollständig integrierte Teilsysteme erweitert. Die Erfassung von Flächendaten erfolgt in einem Geografischen Informationssystem. Nebst den Direktzahlungen unterstützt GELAN unter anderem nachfolgende Vollzugsbereiche: Strukturverbesserungen, Ressourcenprojekte, Naturschutz, Tierschutz, Tierseuchenrecht, Gewässerschutz und Kontrollwesen. Insgesamt über 30 000 Bewirtschaftende und rund 500 Mitarbeitende der drei kantonalen Verwaltungen nutzen die GELAN-Fachanwendung für den Agrarvollzug. Jährlich werden rund CHF 1 Milliarde an Subventionen über das GELAN-System abgewickelt. In den nächsten Jahren ist eine Neuentwicklung des seit 1999 in Betrieb stehenden GELAN-Agrarinformationssystems vorgesehen.

Die Prüfungshandlungen konzentrierten sich schwergewichtig auf die nachfolgenden Prüfgebiete: ISDS-Governance, ISDS-Umsetzung und -Betrieb auf Basis der ISDS-Konzeption, Prüfung der nachvollziehbaren Umsetzung der definierten Konzeption (ISDS-Soll) im ISDS-Ist, das GELAN-Berechtigungsmanagement, die Datenhaltung und die Schnittstellen sowie die externen Dienstleistungen und das Outsourcing.

Bei der Prüfung wurden über alle Prüfbereiche hinweg Verbesserungsmöglichkeiten festgestellt, u. a. eine optimierungsfähige ISDS-Steuerung (fehlende oder unvollständige Dokumente wie ISDS-Strategie, Risikomanagement etc.). Die Datenarchitektur war im Weiteren nur unvollständig dokumentiert. Operativ wurden umfangreiche Administratoren-Berechtigungen festgestellt, es bestehen

Lücken und Unklarheit in Bezug auf die ISDS-Anforderungen bei der Softwareentwicklung und dem Softwaretesten des GELAN-Agrarinformationssystems. Die Prüfung erfolgte in enger Zusammenarbeit mit der FK in einem freundlichen und aufgeschlossenen Umfeld.

Grundversorgungsservice «BE-Web»

Das KAIO ist das Kompetenzzentrum des Kantons Bern für ICT und die Digitalisierung. Der Service «BE-Web», welcher für die Verwaltung der öffentlichen Internet-Webseiten der kantonalen Verwaltung ein aktuelles Content Management System zur Verfügung stellt, wurde Ende 2021 im Rahmen eines Projekts eingeführt. Der Betrieb der technischen Plattform erfolgt bei der Bedag. Die Dienstleistungen für die Integration und Umsetzung sowie den fachlichen Betrieb der BE-Web-Plattform bezieht das KAIO extern. Zudem werden Dienste zur Analyse und Verbesserung der Webseiten, für Suchfunktionen und für die Darstellung von integrierten Bildern von Cloud-Dienstleistern bezogen. Dabei stellt das KAIO den Direktionen im Rahmen von BE-Web die technische Basisinfrastruktur sowie einen fachlichen Basismandanten zur Verfügung, damit die Direktionen ihre dezidieren Internetauftritte in eigener Verantwortung verwalten können.

Die Prüfungshandlungen fokussierten sich auf die Einhaltung des ICT-Grundschutzes und der Anforderungen bei erhöhtem Schutzbedarf mit Blick auf Normen und Rahmenwerke wie ISO/IEC 27001, 27701 bzw. BSI-Grundschutz. Geprüft wurden weiter die umgesetzten Massnahmen betreffend die verlangte ISDS-Steuerung, die ISDS-Aufgaben und -Prozesse, die fachliche und technische Basisinfrastruktur sowie die zugehörige Organisation.

Im Rahmen der Prüfung mussten in zahlreichen Bereichen Befunde mit hoher und mittlerer ISDS-Risikoeinschätzung festgestellt werden. So bestand Unklarheit bei der ISDS-Verantwortung und -Steuerung, und die Übergabe des Projekts in den ordentlichen Betrieb wurde nicht nachvollziehbar umgesetzt. Weiter wurden im Projekt festgehaltene ISDS-Aufgaben nicht wahrgenommen bzw. ausgeführt (u. a. ein weitreichender Sicherheitstest vor der Betriebsaufnahme). Grundlagendokumente wie die Schutzbedarfs- und die Risikoanalyse, das ISDS- und das Berechtigungskonzept mit den Soll-Vorgaben sowie den ISDS-Massnahmen waren unvollständig und nicht aktuell. Die netzwerktechnische Einbindung der produktiven BE-Web-Betriebsplattform wies zudem Mängel auf. Die Prüfung erfolgte in guter Zusammenarbeit und Einvernehmen mit der geprüften Stelle.

Grundversorgungsservice «BE-Applikationsplattformen»

Mit dem KAIO-Service Applikationsplattformen (APF) wird den Direktionen eine zentrale und standardisierte Plattform zur Verfügung gestellt, welche als technische Grundlage für die Fach- und Konzernapplikationen

(Anwendungssoftware) dient. Im Allgemeinen wird diese Form von ICT-Dienstleistung als «Platform as a Service» (PaaS) bezeichnet. PaaS ist eine Art des Cloud-Computings,
bei der die technische Anwendungssoftware-Plattform von einem Drittanbieter zur Verfügung gestellt wird. Der Kanton Bern hat im Rahmen eines Projekts über 200 Fachanwendungen von den dezentralen ICT-Systemen der Direktionen auf die zentralisierte APF-Plattform migriert.

Das Prüfgebiet umfasste die Beurteilung der Einhaltung des ICT-Grundschutzes und der Anforderungen bei erhöhtem Schutzbedarf in Bezug auf Normen und Rahmenwerke wie ISO/IEC 27001, 27701 bzw. BSI-Grundschutz, die implementierten ISDS-Massnahmen bei wesentlichen Prozessen und Aufgaben, der Betrieb der APF-Plattform, die ICT-Infrastruktur, die Leistungsverträge und die verantwortlichen internen und externen Organisationen.

Die Prüfung ergab vor allem eine ungenügende Kontrolle des Vollzugs von vertraglich vereinbarten Aufgaben. So musste festgehalten werden, dass ISDS-Vorgaben bei der Migration der Fachanwendungen nicht eingehalten und die Umsetzung nicht kontrolliert wurde. Notwendige ISDS-Dokumente fehlten oder waren nicht transparent einsehbar. Zudem wurden der Betreiberin der APF-Plattform keine spezifischen ISDS-Anforderungen aus den Fachanwendungen kommuniziert. Die fehlende Sichtbarkeit der Summe aller ISDS-Anforderungen kann sich dabei negativ auf die APF-Plattform auswirken. Die Prüfung erfolgte in einem professionellen und kooperativen Umfeld.

Konzernfachanwendung «SAP/ERP»

Der Kanton Bern führte per 2023 SAP/ERP als führendes Finanz- und Personalbewirtschaftungssystem ein und löste damit die bisherigen Konzernfachanwendungen FIS (Finanz- und Rechnungswesen) und PERSISKA (Personalverwaltungssystem und Gehaltsbuchhaltung) ab. Im Jahr 2020 startete die Realisierungsphase, im Herbst 2021 begann sodann die Einführungsphase. Der Go-Live-Entscheid wurde schliesslich im Dezember 2022 gefällt. SAP bietet professionelle Softwarelösungen für ERP und Software für unternehmensspezifische Prozesse mittelständischer Unternehmen. Ein SAP-System stellt eine komplexe Softwarelösung für sämtliche Geschäftsprozesse im Unternehmen dar. SAP steht als Begriff und Abkürzung für Systeme, Anwendungen, Produkte in der digitalen Datenbearbeitung.

Zum Zeitpunkt der Prüfungshandlungen befand sich das SPA/ERP-System noch nicht im produktiven Betrieb. Dennoch konnten eingeschränkte Prüfungshandlungen in Bezug auf die ISDS-Governance, die ISDS-Konzeption, das Berechtigungsmanagement, die Datenhaltung und die Schnittstellen sowie die externen Dienstleistungen und das Outsourcing durchgeführt werden.

Die Prüfung ergab, dass grundlegende ISDS-Aspekte wie eine verbindliche und abgestimmte ISDS-Governance inkl. Risiko-/Security-Management und -Konzeptionen noch nicht vollständig bestanden bzw. noch umfangreiche Pendenzen enthielten. Zudem war das Berechtigungsmanagement noch wenig umfassend festgelegt. Die Prüfung erfolgte in enger Zusammenarbeit mit der FK in einer kooperativen und freundlichen Umgebung.

Schengener Informationssystem Kantonspolizei Bern

Mit der Übernahme des Schengen-Acquis verpflichtete sich die Schweiz zu gewährleisten, dass eine unabhängige Behörde die Rechtmässigkeit der Verarbeitung von personenbezogener Daten im Schengener Informationssystem (SIS) in ihrem Hoheitsgebiet und deren Übermittlung aus ihrem Hoheitsgebiet überwacht. Die kantonalen Datenschutzbehörden sind somit angehalten, periodisch die Rechtmässigkeit der Bearbeitung personenbezogener SIS-Daten zu überprüfen.

Die DSA prüfte im Berichtsjahr die SIS-Zugriffe von Mitarbeiterinnen und Mitarbeiter der Regionalpolizei Mittelland-Emmental-Oberaargau. Die Prüfziele umfassten die SIS-Nutzung aufgrund von systemtechnischen Aufzeichnungen der SIS-Zugriffe und das Datenschutzbewusstsein der involvierten Mitarbeiterinnen und Mitarbeiter.

Im Umgang mit der SIS-Nutzung und den Abfrageergebnissen empfahl die DSA Optimierungen: Mit regelmässiger Schulung und/oder Information sollen die spezifischen datenschutzrechtlichen SIS-Anforderungen im Umgang mit Personendaten bei SIS-Abfragen vermittelt, bestehende Kenntnisse vertieft und die Sensibilisierung für den datenschutzkonformen Umgang mit dem SIS-Informationssystem gestärkt werden. Neue Mitarbeitende sollten zeitnah und in geeigneter Weise in die SIS-Nutzung eingeführt werden. Die Prüfung erfolgte in einem freundlichen und hilfsbereiten Umfeld.

6.5 Weitere aufsichtsrechtliche Instrumente

6.5.1. 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.

6.5.2. 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 gelangten auch im Berichtsjahr zahlreiche Anfragen zu kommunalen Angelegenheiten an die DSA, sei es direkt von Gemeindebehörden

(die teils gar nicht wussten, dass sie eine eigene Aufsichtsstelle haben), sei es von kommunalen Aufsichtsbehörden (oder auf deren Empfehlung von den Ratsuchenden). Wiederkehrende Fragen betrafen die ISDS-Anforderungen bei der Einführung von Microsoft 365, den Erlass von kommunalen Datenschutzreglementen oder Berechtigungsregelungen für die GERES-Plattform des Kantons sowie die Videoüberwachung im öffentlichen Raum bzw. in öffentlichen Einrichtungen.

Im Rahmen der laufenden Revision des KDSG soll eine im Rahmen einer informellen Arbeitsgruppe mit Beteiligung des AGR, des Verbands Bernischer Gemeinden, Vertreterinnen und Vertretern von Gemeinden verschiedener Grössen sowie der Regierungsstatthalter erarbeitete Neuregelung zur Diskussion gestellt werden. Diese sieht vor, dass die Datenschutzberatung und Aufsicht auch in kommunalen Angelegenheiten auf die DSA übertragen werden und nur noch die vier grössten Gemeinden über eine eigene Datenschutzbehörde verfügen würden.

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, wobei im Frühling der Jubiläumsanlass zum 20-jährigen Bestehen von privatim nachgeholt werden konnte, welche 2020 pandemiebedingt verschoben werden musste. Der Vorstand und dessen Ausschuss verfassten zu neun Vernehmlassungen des Bundes Stellungnahmen von privatim und teils zusätzlich Mustervorlagen für die Mitglieder. Im Austausch mit dem EDÖB wurden Fragen der Aufsichtszuständigkeit beim Beizug von privaten Datenbearbeitern durch kantonale und kommunale Behörden sowie bei öffentlichen und privaten Organisationen, die sowohl privatrechtlich als auch hoheitlich handeln, besprochen. Privatim unterstützte die Organisation «Digitale Verwaltung Schweiz» beim Aushandeln besserer Datenschutzregelungen im erneuerten Rahmenvertrag der SIK mit Microsoft für den Bezug von Cloud-Services durch öffentliche Organe, unterzog einen ersten Entwurf der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) für ein interkantonales Zusammenarbeits- und Datenaustauschkonkordat einer fachlichen Review und setzte sich dafür ein, dass die eOperationsAG im Zusammenhang mit dem Service «eUmzug» ihre Informationspflichten gegenüber den umzugswilligen Personen korrekt erfüllt. Einen institutionalisierten Austausch pflegt privatim zur Fachagentur Educa, welche im Auftrag der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren mehrere Projekte im Bildungsbereich durchführt, welche auch den Datenschutz betreffen.

Um deren Arbeit zu erleichtern, informierte die DSA die interessierten Mitglieder von privatim über ihre auch für diese massgeblichen Feststellungen aus der Vorabkontrolle der vom Bund zur Führung der kantonalen Krebsregister zur Verfügung gestellten Software. In anderen Fällen ist es die DSA, welche von Vorarbeiten einer anderen Aufsichtsstelle profitieren kann.

Arbeitsgruppen von privatim

Die *Arbeitsgruppe Digitale Verwaltung* und eine dafür eingesetzte Unterarbeitsgruppe boten einen ersten Workshop zum Thema «Meldung von Datenschutzvorfällen» («Data Breach Notification») an. Der gut besuchte Workshop befasste sich mit Aspekten der Kritikalität/Risiken, der Massnahmen, der Information der Betroffenen sowie des Meldeprozesses und führte zu aufschlussreichen Erkenntnissen für die Praxis in den Kantonen. Gestützt darauf werden nun die bestehenden Hilfsdokumente für die Kantone überarbeitet und aktualisiert.

Die *Arbeitsgruppe Sicherheit* traf sich zu zwei Arbeitssitzungen, um gemeinsam Fragen zur polizeilichen Überwachung mit technischen Hilfsmitteln, zum interkantonalen Datenaustausch im Polizeibereich und zu weiteren Datenschutzaspekten im Polizei- und Justizwesen zu erörtern. Auf Anfrage der KKPKS prüfte sie zwei Entwurfsfassungen für ein Datenaustauschkonkordat, einmal zuhanden der formellen Stellungnahme von privatim und einmal zuhanden einer informellen Rückmeldung zum überarbeiteten Entwurf.

Die *Arbeitsgruppe Gesundheit* tagte im Berichtsjahr viermal, jeweils abwechslungsweise virtuell und physisch vor Ort. Der Austausch unter den auf den Datenschutz im Gesundheitswesen spezialisierten Mitgliedern fokussierte sich erneut auf wichtige datenschutzrechtliche Fragestellungen «post-Pandemie» (insbes. zur Aufbewahrung und Löschung von Kontaktdaten sowie zu den Erkenntnissen im Hinblick auf eine Revision des EpG). Zudem wurde der Austausch über das Elektronische Patientendossier (EPD) intensiviert; diskutiert wurde etwa, wie es um ein angelegtes Dossier für ein Kind steht, wenn dieses urteilsfähig bzw. volljährig wird. Das Thema EPD wird auch im Folgejahr weiterbearbeitet

In der *Arbeitsgruppe IC*T besprachen Vertreter/innen der Kantone, deren Aufsichtsstellen über Spezialistinnen und Spezialisten für Informationssicherheit verfügen, aktuelle technische Fragen.

7 Antrag

Kenntnisnahme.

8 Glossar / Abkürzungen

ABEV	Amt für Bevölkerungsdienste
Abs.	Absatz
AFV	Automatisierte Fahrzeugfahndung und Verkehrsüberwachung
AGR	Amt für Gemeinden und Raumordnung
AHV	Alters- und Hinterlassenenversicherung
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
AIS	Amt für Integration und Soziales
AJV	Amt für Justizvollzug
AKVB	Amt für Kindergarten, Volksschule und Beratung
APF	Applikationsplattform
Art.	Artikel
AVA	Amt für Arbeitslosenversicherung
BE-GEVER	Elektronische Geschäftsverwaltung (der Kantonsverwaltung)
BKD	Bildungs- und Kulturdirektion
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
Bst.	Buchstabe
DIJ	Direktion für Inneres und Justiz
DSA	Datenschutzaufsichtsstelle des Kantons Bern
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
DSV	Datenschutzverordnung
DVG	Gesetz über die digitale Verwaltung
DVV	Verordnung über die digitale Verwaltung
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

EPD	Elektronisches Patientendossier
EpG	Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz)
ERP	Enterprise Resource Planning
EU	Europäische Union
FIN	Finanzdirektion
FK	Finanzkontrolle
GELAN	Gesamtlösung EDV Landwirtschaft & Natur
GERES	Gemeinderegistersystem
GERES V	Verordnung über die Gemeinderegistersysteme-Plattform
GSI	Gesundheits-, Sozial- und Integrationsdirektion
ICSG	Gesetz über die Informations- und Cybersicherheit
ICT	Informations- und Telekommunikationstechnik
IMG	Gesetz über die Information und die Medienförderung
ISDS	Informationssicherheit und Datenschutz
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Informatik
JVG	Gesetz über den Justizvollzug (Justizvollzugsgesetz)
KAIO	Amt für Informatik und Organisation
KAPO	Kantonspolizei
KDSG	(Kantonales) Datenschutzgesetz
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KKPKS	Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz
M365	Microsoft 365

ORS	ORS Service AG
PaaS	Platform as a Service
PDSG	Gesetz über die zentralen Personendatensammlungen (Personendatensammlungsgesetz)
PG	Personalgesetz
PolG	Polizeigesetz
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
RDV	Randdatenverordnung
SID	Sicherheitsdirektion
SIK	Schweizerische Informatikkonferenz
SIS	Schengener Informationssystem
SORMAS	Surveillance and Out-break Response Management System
SPS	Swiss Post Solutions
SRO	Spital Region Oberaargau
STA	Staatskanzlei
StAB	Staatsarchiv
SV	Steuerverwaltung
SVSA	Strassenverkehrs- und Schifffahrtsamt
TCHF	Tausend Franken
UPD	Universitäre Psychiatrische Dienste Bern
VE	Vorentwurf
VRPG	Gesetz über die Verwaltungsrechtspflege
WEU	Wirtschafts-, Energie- und Umweltdirektion

Ziff.	Ziffer
ZPV V	Verordnung über die Zentrale Personenverwaltung

Datenschutzaufsichtsstelle
des Kantons Bern

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

www.be.ch/dsa