Kanton Bern
Canton de Berne

# Jahresbericht Datenschutzaufsichtsstelle 2020

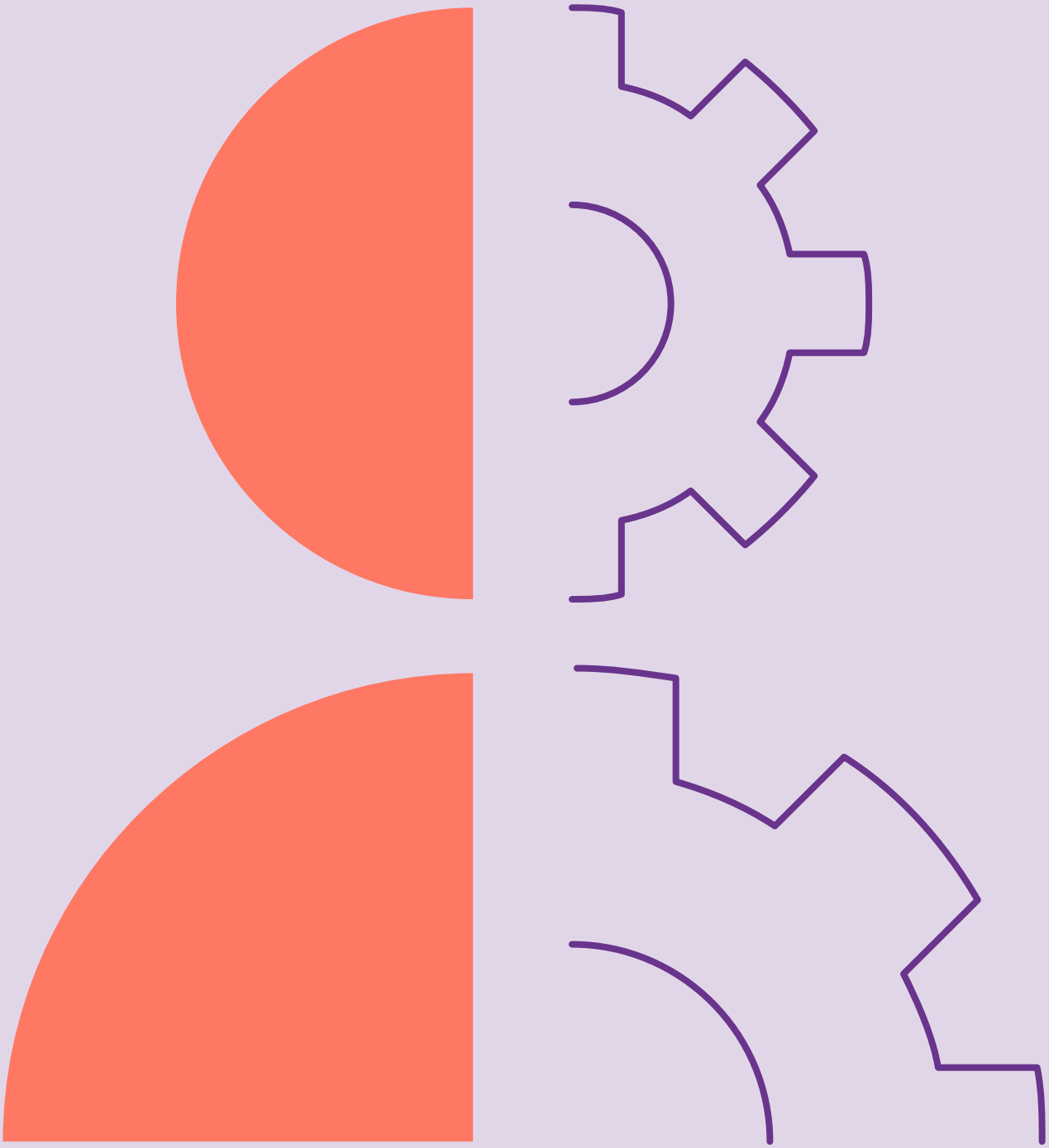
Datenschutzaufsichtsstelle

Februar 2021

**Impressum**

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

Layout und Realisation: noord.ch



# 1 Vorwort

Eigentlich hoffte die DSA nach zahlreichen personellen und fachlichen Neuerungen im Vorjahr auf ein «normales» Jahr 2020, welches nebst der ordentlichen Erfüllung ihrer Aufgaben auch zur weiteren Konsolidierung der internen Organisation und Arbeitsmittel sowie externen Kontakte genutzt werden konnte. Doch dann kam Corona …

Weil die DSA überwiegend auf der Grundlage von elektronischen Dokumenten arbeitet und praktisch alle Anfragen von betroffenen Personen per E-Mail oder Telefon eingehen, brachten die Monate der empfohlenen bzw. angeordneten Heimarbeit keine grundlegenden Schwierigkeiten für die Aufgabenerfüllung. Lediglich die Prüfungen der Informationssicherheit und des Datenschutzes von in Betrieb stehenden Systemen (Audits), welche üblicherweise bei der geprüften Stelle vor Ort stattfinden, wurden dadurch erschwert oder eingeschränkt, dass teils mit Besprechungen oder Interviews per Telefon gearbeitet werden musste.

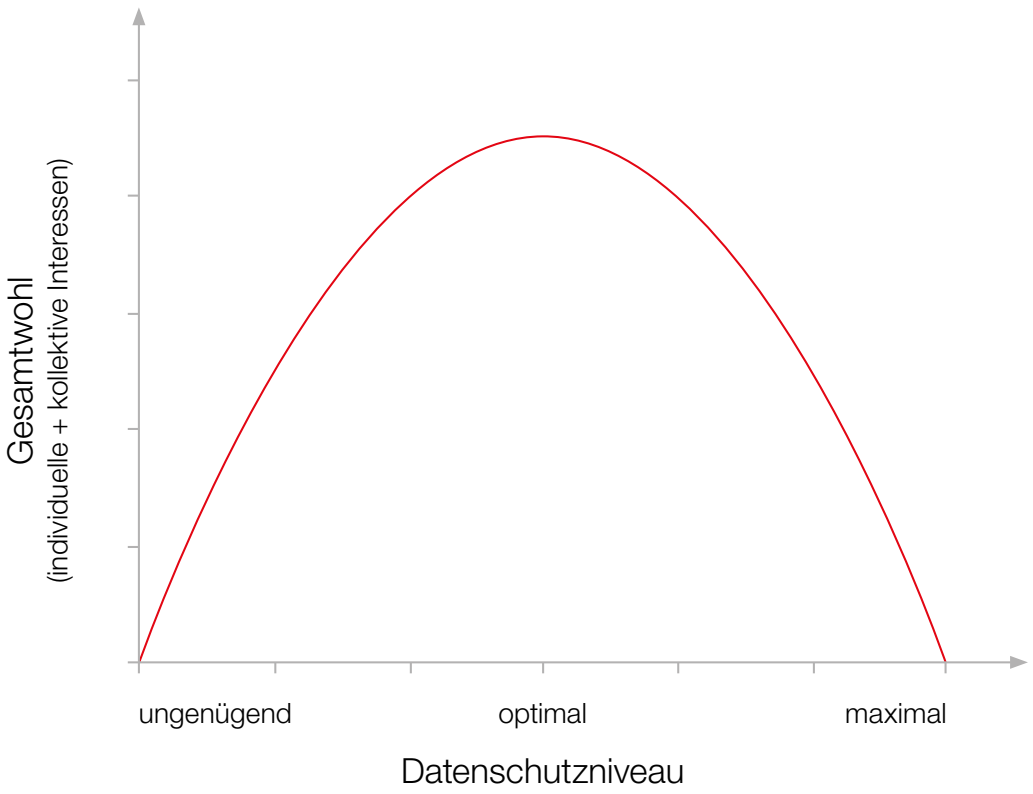
Die besondere Herausforderung lag darin, dass sich mit den Massnahmen des Bundes und des Kantons zur Eindämmung der Pandemie und zur Abfederung derer Auswirkungen auf das gesellschaftliche und wirtschaftliche Leben sehr plötzlich viele neue datenschutzrechtliche Fragen stellten, auf die sich die beteiligten Behörden – die ihrerseits unter enormem Druck standen – und betroffene Personen (sowie auch die Medien) möglichst bald eine Antwort wünschten. Dabei wurde manchmal auch das Datenschutzrecht als solches in Frage gestellt, soweit darin ein Hindernis für schnelles und wirkungsvolles behördliches Handeln gesehen wurde. Hier galt es nebst der fachlichen Beratung auf die folgenden Aspekte hinzuweisen: Unser Rechtsverständnis beruht auf dem Grundsatz der – auch informationellen – Selbstbestimmung der Bürger*innen. Deren Rechte und Freiheiten dürfen zur Wahrung von öffentlichen Interessen wie dem Schutz der Gesundheit eingeschränkt werden, dabei sind aber immer die grundlegenden rechtsstaatlichen Prinzipien, insbesondere die Gesetz- und Verhältnismässigkeit jedes staatlichen Handelns, einzuhalten. Deshalb dürfen die Behörden nicht plötzlich nach eigenem Gutdünken alle ihnen nützlichen Personendaten sammeln und untereinander austauschen, andernfalls finden wir uns auf einmal in einem Überwachungsstaat wieder, vor dem uns das Datenschutzrecht gerade schützen soll. Dieses ist dank auslegungsfähigen Begriffen wie der Wahrung von «überwiegenden Interessen», der «Verhältnismässigkeit» von Datenbearbeitungen und der «Angemessenheit» von Massnahmen zur Wahrung der Informationssicherheit durchaus in der Lage, auch in ausserordentlichen Situationen passende Antworten zu liefern.

Ueli Buri, Datenschutzbeauftragter

# 2 Grundrecht auf Datenschutz

Der Schutz der Privatsphäre einschliesslich des Schutzes vor Missbrauch der persönlichen Daten 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.



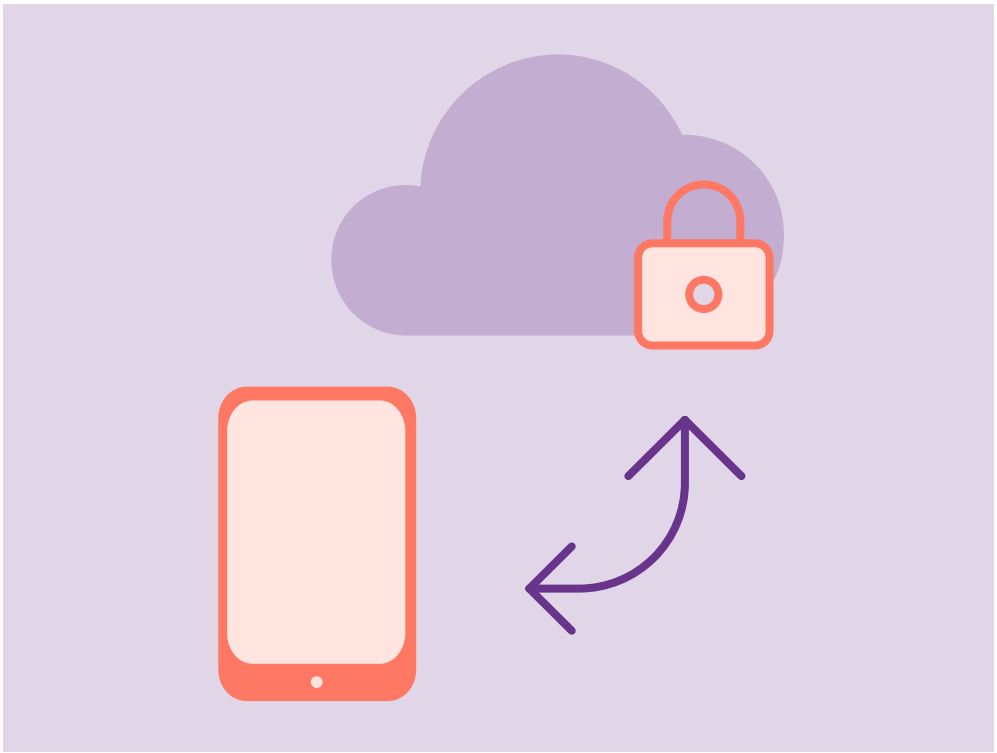
Das Datenschutzgesetz konkretisiert die Pflichten der Behörden beim Bearbeiten von Personendaten, wobei nebst der Verwaltung auch weitere Träger von öffentlichen Aufgaben, z.B. Schulen und Spitäler, als Behörden gelten. Dabei umfasst «Bearbeiten» jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren,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

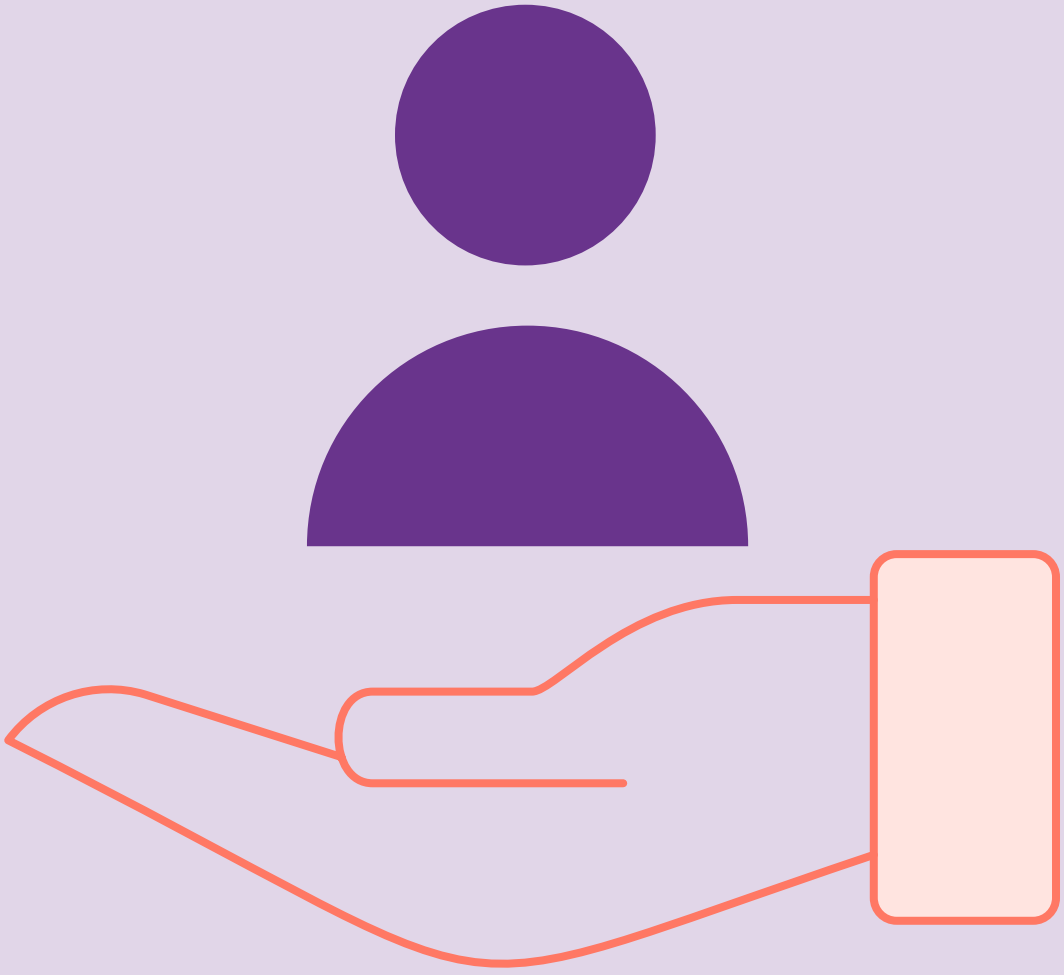
# 3 Verantwortung und Aufsicht

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 kantonale Datenschutzgesetz (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 – 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 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 2020 verfügte die DSA über einen Personalbestand von 510 % (bei einem bewilligten Bestand von 515 %), aufgeteilt auf sieben Personen. Davon sind fünf Personen juristisch ausgebildet, zwei Personen sind Informatiker bzw. Informatikprüfer:

**Ueli Buri** (Datenschutzbeauftragter) leitet die DSA seit dem 1. März 2019. Er verantwortet die Festlegung der strategischen Ausrichtung und jährlichen Leistungsziele der DSA sowie deren personelle und betriebliche Führung. Fachlich betreut er primär drei Direktionen (Bau und Verkehr, Inneres und Justiz, Sicherheit), die Staatskanzlei 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 sämtlichen Videoüberwachungen und bei Fragen von Kirchgemeinden.

**Daniel Stucki** (Wissenschaftlicher Mitarbeiter Recht) ist Rechtsanwalt und seit 2008 in der Informatikbranche tätig. In der DSA ist er seit Anfang 2019 und hauptsächlich zuständig für Auskünfte und Beratung sowie Vorabkontrollen in den Bereichen Gesundheit und Bildung.

**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.

Im Jahr 2020 betrug der Betriebsaufwand der DSA insgesamt TCHF 153 (Budget: TCHF 168). Davon wurden ca. 80 % (TCHF 122) für externe Dienstleistungen zur Unterstützung von Informatikprüfungen eingesetzt (die letzte Prüfung des Berichtsjahres wurde erst im nachfolgenden Januar fakturiert und wird deshalb das Rechnungsjahr 2021 belasten).

Innerhalb der kantonalen Verwaltung bestehen weitere Anlaufstellen, welche die verantwortlichen Behörden in ISDS-Fragen beraten: So verfügen die Direktionen und die Staatskanzlei 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 fachspezifische Fragen (z.B. betreffend die Digitalisierung der Volksschule) an die Direktionen und die Staatskanzlei 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. 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 und Insel Gruppe AG).

Im Hinblick auf einen gesamtstaatlich abgestimmten ISDS-Auditplan prüfen die Finanzkontrolle des Kantons Bern (FK) und die DSA eine verstärkte strategisch ausgerichtete Zusammenarbeit.

Als Mitglied von «privatim», der Konferenz der schweizerischen Datenschutzbeauftragten, pflegt die DSA den 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 eine Person der DSA teil. Siehe für Einzelheiten zu den im Berichtsjahr bearbeiteten Themen unter Ziff. 6.7 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 «Corona»

Die Massnahmen des Bundes und des Kantons zur Bekämpfung der Corona-Pandemie und zur Abfederung derer Auswirkungen auf das gesellschaftliche und wirtschaftliche Leben beschäftigten die DSA ab März 2020 sehr regelmässig und in unterschiedlichen Bereichen ihrer Tätigkeiten. Sie bildeten damit ein Schwerpunktthema, zu dem hier vorweg und aufgabenübergreifend berichtet werden soll.

### 6.1.1 Beratung Behörden

**covidtracker.ch**

Die anfänglich von Privatpersonen erstellte und später von der ETH Zürich betreute Plattform covidtracker.ch, welche auf der Grundlage von anonymen Angaben zur Entwicklung von Corona-Symptomen Daten für die epidemiologische Beobachtung und die Aufbereitung von Statistiken liefern sollte, wurde von der Gesundheits- und Integrationsdirektion (GSI) öffentlich empfohlen. Mindestens von einer datenschutzrechtlichen Mitverantwortung der GSI ausgehend, empfahl die DSA, auf die zwingende Angabe der letzten vier Ziffern der Telefonnummer zu verzichten, weil diese zusammen mit dem Geburtsjahr und der Postleitzahl des Wohnortes eine Re-Identifikation der Teilnehmenden ermöglichen können.
In der Folge wurde die Telefonnummer entfernt, zumal diese den beabsichtigten Zweck (Erkennen und Zuordnen von Mehrfacheingaben der gleichen Personen) nicht erfüllte.

**Publikation Infektionszahlen pro Gemeinde**

Während der Zeit, als die Fallzahlen die entsprechende Aufbereitung noch zuliessen, begann die GSI mit der Publikation der täglichen Neuansteckungen pro Gemeinde im Internet. Für Kleinstgemeinden hielt die DSA diese Publikation für problematisch, weil dort die Möglichkeit bestand, die Erkrankung einer bestimmten Person zuzuordnen. Die DSA empfahl der GSI deshalb dringend, in jenen Fällen auf eine namentliche Angabe der Gemeinde zu verzichten. Die GSI setzte die Empfehlung um und publizierte ab dann nur noch Informationen im Sinne von «Kleinstgemeinde im Verwaltungskreis …».

### Merkblatt «Home-Office» für das Kantonspersonal

Während des ersten Lockdown im März 2020 erarbeitete das Amt für Informatik und Organisation (KAIO) ein Merkblatt mit technischen Tipps und Tricks für Mitarbeitende im Home-Office. Auf Empfehlung der DSA wurde auch ein Abschnitt über den Datenschutz zuhause in das Merkblatt aufgenommen. Im von der DSA verfassten Text wird das Personal darauf hingewiesen, dass das Amtsgeheimnis auch gegenüber Familienangehörigen gilt und deshalb Dokumente und Besprechungen auch zuhause vertraulich behandelt werden müssen. Anders als im Büro, wo die Entsorgung geregelt verläuft, dürfen Geschäftsdokumente nicht einfach ins Altpapier gelegt werden. Für Situationen, in denen nicht die kantonale Software «Skype for Business» eingesetzt werden kann, verweist das Merkblatt auf eine von der Datenschutzbeauftragten des Kantons Zürich zusammen mit der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) erstellten Liste von Videokonferenzlösungen, welche während der Corona-Krise «einigermassen datenschutzkonform» genutzt werden können.

## 6.1.2 Beratung betroffene Personen

### Erhebung von Kontaktdaten in Restaurants

Die vorgeschriebene Erhebung von Kontaktdaten in Restaurants führte zu zahlreichen Anfragen von betroffenen Personen. Sie erkundigten sich insbesondere nach der Zulässigkeit der Erhebung des Geburtsdatums oder beschwerten sich über die Verwendung von Listen, aus denen auch die Angaben der anderen Gäste ersichtlich waren. Als erste Anlaufstelle beantwortete die DSA auch Anfragen, welche das für private Betriebe geltende Datenschutzrecht des Bundes betrafen, und informierte danach den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) als zuständige Behörde über ihre Antworten.

Die Erhebung des Geburtsdatums ist in einer Verordnung, welche der Kanton Bern gestützt auf das Epidemiengesetz des Bundes erliess, ausdrücklich verankert. Laut der Gesundheits- und Integrationsdirektion (GSI) ist das Geburtsdatum in einzelnen Fällen zur eindeutigen Identifikation des Gastes erforderlich. Die DSA wies die GSI mehrmals darauf hin, dass erst eine genügende Anzahl von solchen Fällen eine flächendeckende Erhebung rechtfertige, und empfahl, bei einer nächsten Überprüfung der Angemessenheit der Massnahmen – welche das Bundesrecht vorschreibt – insbesondere diesen Punkt genau zu verifizieren und gegebenenfalls zu korrigieren.

Die Erhebung von Kontaktdaten direkt in Listen ist datenschutzrechtlich klar unzulässig. Deshalb schreibt die betreffende Verordnung des Bundesrates vor, dass die Vertraulichkeit der Daten bei der Erhebung zu gewährleisten ist. Die GSI stellt auf ihrer Webseite Excel-Listen zur Verfügung, welche für die betriebsinterne

Zusammenstellung der Kontaktdaten und ggf. Übermittlung an das Kantonsarztamt verwendet werden können, nicht aber zur Datenerfassung durch die Gäste selbst. Auf Empfehlung der DSA hin stellte die GSI dies auf der betreffenden Webseite eindeutig klar.

### 6.1.3 Formelle Stellungnahmen

#### Verordnung über Unterstützungsmassnahmen im Kultursektor

Für die Umsetzung und den Vollzug der COVID-Verordnung Kultur des Bundes war eine entsprechende kantonale Verordnung zu erlassen. Die Richtlinien des Bundesamtes für Kultur sahen vor, dass die Gesuchsteller*innen für Unterstützungsleistungen den für die Behandlung ihrer Gesuche nötigen Datenbekanntgaben an Dritte zustimmen sollten. Die zum kantonalen Verordnungsentwurf konsultierte DSA sah in der gesetzlichen Verpflichtung der Gesuchsteller*innen zur Erteilung einer Zustimmung aber ein seltsames Konstrukt: Damit die Zustimmung einer betroffenen Person datenschutzrechtlich wirksam sein kann, muss sie freiwillig erfolgen. Es erschien der DSA – und in der Folge auch der Bildungs- und Kulturdirektion (BKD) – als sinnvoller und transparenter, für die nötigen Datenbekanntgaben direkt in der Verordnung eine Rechtsgrundlage zu schaffen und die Gesuchsteller*innen lediglich angemessen darüber zu informieren.

#### Verordnung über Massnahmen im Bereich der familienergänzenden Kinderbetreuung

Während der ausserordentlichen Lage erliess der Regierungsrat direkt gestützt auf die Kantonsverfassung eine Regelung zur finanziellen Unterstützung der Kinderbetreuung in Kindertagesstätten und Tagesfamilien. Für den korrekten Vollzug des Lastenausgleichs musste berücksichtigt werden, inwieweit ihre Kinder abgebende Eltern bereits Sozialhilfebeiträge erhalten, wobei Angaben zu Leistungen der Sozialhilfe als besonders schützenswerte Personendaten gelten. Deren Bearbeitung und insbesondere Bekanntgabe muss im Gesetz ausdrücklich vorgesehen werden. Auf Antrag der DSA wurde deshalb in der Verordnung statuiert, dass das Amt für Integration und Soziales (AIS) Personendaten über die Sozialhilfe bei den betreffenden Leistungserbringern einholen darf. Ein erster Vorschlag, wonach die beteiligten Institutionen solche Daten «austauschen» dürfen, erachtete die DSA als zu weitgehend, weil der Informationsfluss klar nur in einer Richtung erforderlich war.

### Verordnung über Massnahmen zur Bekämpfung der Covid-19-Epidemie

Gestützt auf das einschlägige Bundesrecht schrieb der Kanton Bern zunächst nur für Barbetriebe und Diskotheken eine Erfassung der Kontaktdaten ihrer Gäste vor, wobei über die Bundesvorgaben hinaus auch eine Mobiltelefonnummer und eine E-Mail-Adresse verlangt wurden, um die Personen bei Bedarf sehr schnell kontaktieren zu können. Einen Monat später wurde die zwingende Kontaktdatenerfassung auch auf alle Restaurationsbetriebe ausgedehnt, nachdem Kontrollen der Schutzmassnahmen ergeben hatten, dass in zu vielen Fällen Unsicherheiten bestanden und die getroffenen Massnahmen nicht genügten; eine Erhebung von Mobiltelefonnummern und E-Mail-Adressen wurde hier nicht vorgesehen. Die DSA erachtete sowohl die Ausdehnung der Kontaktdatenerfassung als auch die Differenzierung bei den erfassten Daten für verhältnismässig: Restaurants werden von breiteren Bevölkerungskreisen (auch von Personen ohne Handy bzw. E-Mail) besucht, und der Kontakt zwischen den Gästen erfolgt kontrollierter als in Bars und Diskotheken. Als fraglich erschien der DSA aber, ob zusätzlich zur vollständigen Adresse tatsächlich auch das Geburtsdatum erhoben werden muss (siehe dazu Ziff. 6.1.2 oben).

## 6.1.4 Vorabkontrollen

### Fachapplikation SORMAS für das Contact Tracing

Die Applikation «Surveillance and Outbreak Response Management System» (SORMAS) wird von diversen Kantonen zum Zweck des Contact Tracing eingesetzt – so auch vom Kanton Bern. Die für SORMAS verantwortlichen Behörden der Gesundheits- und Integrationsdirektion (GSI) informierten die DSA auf deren Rückfrage hin im Mai 2020 darüber, dass SORMAS im Kanton zur Anwendung gelangen werde. Kurz darauf brachten sie der DSA zur Kenntnis, dass sie noch im selben Monat den Testbetrieb mit produktiven Personendaten aufnehmen würden und die Applikation im September 2020 in den definitiven Betrieb übergeben werde. Bis zum Redaktionsschluss des vorliegenden Jahresberichts hat die DSA von den verantwortlichen Behörden keine ISDS-Dokumentation zur Vorabkontrolle erhalten. Die Datenschutzkonformität von SORMAS bleibt somit vorderhand unklar, was angesichts der besonders schützenswerten Personendaten in SORMAS als sehr problematisch erscheint.

# 6.2 Beratung

## 6.2.1 Behörden

### Wiederholung der Abstimmung über die Kantonszugehörigkeit der Gemeinde Moutier

Im Hinblick auf die Wiederholung der Moutier-Abstimmung gelangte die Staatskanzlei (STA) mehrfach an die DSA, um datenschutzrechtliche Fragen frühzeitig zu klären. Das Gesetz betreffend die Durchführung von Abstimmungen über die Kantonszugehörigkeit bernjurassischer Gemeinden ermächtigt den Regierungsrat zu besonderen Massnahmen, um einen reibungslosen Ablauf der Abstimmungen zu gewährleisten. So stellte sich namentlich die Frage, ob der STA ein Zugang zur Gemeinderegistersysteme-Plattform GERES gewährt werden kann, um die Einträge im Stimmregister der Gemeinde Moutier überprüfen zu können. Gestützt auf das vorerwähnte Gesetz erschien dies grundsätzlich als möglich, wobei jedoch für jedes einzelne in GERES enthaltene Attribut darzulegen war, warum es für die Wahrnehmung der Aufgabe erforderlich war. Formell war der neue GERES-Zugang durch eine Ergänzung der Verordnung über die Harmonisierung amtlicher Register zu begründen, in welcher auch alle anderen Berechtigungen der kantonalen Behörden festgelegt sind.

### Einsatz von Microsoft 365 in der Kantonsverwaltung

Der Einsatz von Online-Diensten wie Microsoft 365 führt dazu, dass (Personen-) Daten im Herrschaftsbereich des Dienstleisters – auf dessen Infrastruktur und unter Mitwirkung dessen Personals – bearbeitet werden. Aus Datenschutzsicht liegt eine sog. Auftragsdatenbearbeitung vor, welche voraussetzt, dass die Einhaltung des Datenschutzes und der Datensicherheit auch beim Dienstleister sichergestellt ist, was in einem geeigneten Vertrag zwischen Behörde und Dienstleister zu regeln ist. In einem Rahmenvertrag zwischen der Schweizerischen Informatikkonferenz (SIK) und Microsoft war bislang vorgesehen, dass Verträge über Online-Dienste dem irischen Recht unterstehen und Streitigkeiten (insbes. bei Datenschutzverletzungen) vor irischen Gerichten auszutragen sind. Die Konferenz der schweizerischen Datenschutzbeauftragten (privatim) hielt dies für ungenügend und konnte durch fachliche Beratung der SIK erreichen, dass eine Zusatzvereinbarung neu vorsieht, dass die Datenschutzversprechen im Vertragswerk mit Microsoft – namentlich in deren Data Protection Addendum (DPA) – nach Schweizer Recht ausgelegt werden und im Streitfall vor Schweizer Gerichten durchgesetzt werden können.

Dies bedeutete allerdings nicht, dass die Kantonsverwaltung die Produkte von MS365 nun vorbehaltlos einsetzen konnte. Am 2. Juli 2020 publizierte der

Europäische Datenschutzbeauftragte eine Studie, welche verschiedene weitere datenschutzrechtliche Probleme aufzeigte, welche auch für die Behörden in der Schweiz gelten. Ausserdem erklärte der Europäische Gerichtshof im Entscheid vom 16. Juli 2020 («Schrems II») den *EU-US Privacy Shield* für ungültig, so dass die Übermittlung von Personendaten aus der EU in die USA nicht mehr ohne weiteres zulässig ist; wenig später gelangte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) mit Blick auf den *Swiss-US Privacy Shield* zum gleichen Ergebnis.

Für die Kantonsverwaltung heisst dies, dass vor dem Einsatz eines bestimmten Service – geprüft wird gegenwärtig namentlich die MS Azure Multifaktor Authentifikation – detailliert geprüft werden muss, welche Daten im Einzelnen wo bearbeitet und gespeichert werden, welche Subunternehmer von Microsoft an den Diensten mitwirken und ggf. Zugriff auf Daten haben können, wie die Erhebung und Auswertung von Daten über die Benutzer der Dienste durch Microsoft minimiert werden kann, etc. Sehr erfreulich ist, dass das zuständige Amt für Informatik und Organisation (KAIO) seine Verantwortung hier sehr ernst nimmt und die von der DSA empfohlenen Abklärungen mit der gebotenen Gründlichkeit ausführt.

**Sprachaufzeichnung bei Telefonanrufen**

Ein Spital mit dem Wunsch, Telefongespräche aufzunehmen, wenn Drohungen ausgesprochen werden, wandte sich an die DSA mit der Frage, ob und in welcher Form dies zulässig sei. Nach Auffassung der DSA wäre ein solches Vorgehen datenschutzrechtlich unzulässig und auch strafbar: Grundsätzlich dürfen nichtöffentliche Telefongespräche nur mit Einwilligung der beteiligten Personen aufgezeichnet werden, die Ausnahmen sind im Gesetz vorgesehen. Danach macht sich insbesondere nicht strafbar, «wer als Gesprächsteilnehmer oder Abonnent eines beteiligten Anschlusses Fernmeldegespräche mit Hilfs-, Rettungs- und Sicherheitsdiensten aufnimmt», damit eine rasche und wirkungsvolle Intervention sichergestellt werden kann. Dies war vorliegend jedoch nicht gegeben (es wäre nicht nur die Rettungsnummer betroffen gewesen und der Zweck war nicht die medizinische Intervention). Zudem fehlte aus datenschutzrechtlicher Sicht eine ausreichende Rechtsgrundlage für die beabsichtigte Datenbearbeitung.

### 6.2.2 Betroffene Personen

**Elektronische Datenbearbeitung für Erstellung von Schüler*innenausweise**

Ein Gymnasiast fragte die DSA an, ob eine vom Gymnasium entwickelte App zur elektronischen Einreichung von Fotos für die Erstellung von Schüler*innenausweisen datenschutzkonform betrieben werden könne. Die DSA stellte in

der Folge aufsichtsrechtliche Rückfragen an das betroffene Gymnasium. Nach Klärung des Sachverhalts kam die DSA zum Schluss, dass mit der App eine grössere Anzahl an Fotos von Personen bearbeitet wird. Solche Fotos, namentlich Portraitaufnahmen, gelten als Personendaten. Weil aus ihnen ggf. besonders schützenswerte Informationen (namentlich über die Gesundheit oder die Religion der abgebildeten Person) entnommen werden können, hielt bzw. hält die DSA die Voraussetzungen für eine Vorabkontrollpflicht der App für gegeben. Offenbar war die App ohne vorgängige Vorabkontrolle in Betrieb genommen worden. Soll sie weiterhin genutzt werden, sind die notwendigen ISDS-Unterlagen unverzüglich zu erarbeiten und der DSA zur Prüfung einzureichen. Die DSA wies das Gymnasium auf die Vorabkontrollpflicht hin und erwartet die Unterlagen anfangs 2021.

### Anfragen zur Publikation von Eigentümerdaten im Internet

Seit August 2020 können die im Grundbuch geführten Namen der Eigentümer von jeder Person im Internet eingesehen werden, über das Portal BE-Login ist zudem auch das Geburtsdatum der Eigentümer*innen ersichtlich. Dies führte zu vielen Anfragen von betroffenen Personen, welche jeweils wie folgt beantwortet wurden: Das Zivilgesetzbuch sieht vor, dass jede Person ohne Interessennachweis berechtigt ist, vom Grundbuchamt Auskunft über den Namen und die Identifikation des Eigentümers zu erhalten. In der Grundbuchverordnung (GBV) sind dafür folgende Angaben vorgesehen: Geburtsdatum, Geschlecht sowie Heimatort oder Staatsangehörigkeit. Ferner ermächtigt die GBV die Kantone, die ohne Interessennachweis einsehbaren Daten des Grundbuchs elektronisch öffentlich zugänglich zu machen; sie müssen aber sicherstellen, dass die Daten nur grundstücksbezogen – d.h. insbesondere nicht mittels Suche nach Namen – abgerufen werden können und dass die Auskunftssysteme vor Serienabfragen geschützt sind. Beides ist im Kanton Bern entsprechend umgesetzt worden. Die Öffentlichkeit des Grundbuchs und der Eigentümerschaft ist rechtspolitisch durchaus angezeigt: Grundeigentum verschafft ein ausschliessliches Recht an einem ursprünglich allgemeinen Gut; Eigentümer dürfen ihr Grundstück nutzen und verwerten und Dritte von der Nutzung ausschliessen. Als öffentliches Register schafft das Grundbuch die nötige Transparenz. Wenn Dritte ein fremdes Grundstück nicht betreten dürfen und gegebenenfalls rechtliche Sanktionen erleiden, haben sie das Recht zu wissen, wer ihnen die Einschränkung auferlegt. Zudem gilt – als gesetzliche Fiktion – der gesamte Grundbuchinhalt als bekannt («Die Einwendung, dass jemand eine Grundbucheintragung nicht gekannt habe, ist ausgeschlossen»).

### Beratung und Vermittlung bei eingeschränkter Akteneinsicht bei der Kantonspolizei

Eine betroffene Person gelangte an die DSA, weil sie zwar Einsicht in sie betreffende Einträge im Journal der Kantonspolizei (KAPO) erhalten hatte, die Unterlagen aber zahlreiche geschwärzte Passagen enthielten. Das im Datenschutzgesetz vorgesehene Recht auf Einsicht in die eigenen Daten darf nur eingeschränkt

werden, wenn wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen Dritter entgegenstehen. Als Erklärung für die Schwärzungen gab die KAPO «einsatztaktische Gründe» an. Im Rahmen ihrer Aufgabe der Beratung und Vermittlung zwischen Betroffenen und Behörden liess sich die DSA für jede Schwärzung erklären, welche Art von Information sie betraf. Dabei stellte sich heraus, dass es stets um Angaben ging, die nichts mit der betroffenen Person zu tun hatten, wie die Namen der Polizeibeamt*innen, Fahrzeugnummern und Funkfrequenzen oder auch Angaben zu anderen Personen. Nach Auskunft des Datenschutzverantwortlichen der KAPO ist der Fall sehr selten, dass Angaben zur betroffenen Person selbst abgedeckt werden. Angesichts des gesetzlichen Auftrags der DSA, die Interessen von Personen zu wahren, denen keine oder nur beschränkte Auskunft erteilt werden kann, vereinbarte die DSA mit der KAPO, dass diese die DSA stets vorgängig konsultieren wird, wenn sich ein solcher Fall ereignen sollte.

**Diverse Anzeigen zum Versand von Steuerdaten**

Mehrere Personen wandten sich mit Anzeigen wegen Falschzustellungen von Steuerdaten an die DSA. Weil die Datenschutzverletzung in diesem Zeitpunkt bereits erfolgt war, konnte sie im betroffenen Einzelfall weder verhindert noch rückgängig gemacht werden. Die DSA fragte aber bei den jeweiligen Steuerbehörden konsequent zurück, wie solche Versehen in Zukunft verhindert werden. Dabei zeigte sich, dass die Steuerverwaltung im Fall von Beschwerden oder Anzeigen die Ursachen jeweils korrekt ermittelte und die Fälle zum Anlass nahm, um die internen Prozesse zu prüfen und zu verbessern. Die DSA empfahl den Steuerbehörden zudem, ihre Mitarbeitenden regelmässig für die Wahrung des Steuergeheimnisses im Umgang mit den Steuerdaten zu sensibilisieren.

### 6.2.3 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 – so auch im Berichtsjahr – unterrichten Mitarbeitende der DSA das Fach «Datenschutz und Informationssicherheit» im Rahmen der Lehrgänge zur Erlangung des Fachausweises als Bernische Gemeindefachfrau/Bernischer Gemeindefachmann sowie für Mitarbeitende der Schuladministration. Nebst den allgemeinen Grundsätzen des Datenschutzrechts und deren Anwendung im Fachbereich der Kursteilnehmer*innen ist auch die Diskussion und Beantwortung konkreter Fragestellungen aus dem Arbeitsalltag ein wichtiges Anliegen. Im Jahr 2020 kam erstmals ein Lehrgang für Mitarbeitende von Kirchgemeindesekretariaten dazu. Hier vermittelte die Rednerin der DSA zusätzlich die datenschutzrechtliche Bedeu-

tung der besonderen Bestimmungen im neuen Landeskirchengesetz (LKG) und in den neuen landeskirchlichen Datenschutzreglementen.

### Wissensvermittlung im Rahmen von spezifischen Anlässen

Infolge der Pandemie wurden mehrere geplante Weiterbildungsanlässe von Behörden, zu denen Mitarbeitende der DSA als Redner*innen eingeladen waren, ganz abgesagt oder auf später verschoben. Gleichwohl konnte ein Vertreter der DSA an einem Treffen von Gemeindeschreibern des Verwaltungskreises Thun sowie an einem Weiterbildungsanlass des Gymnasiums Campus Muristalden teilnehmen und Grundlagen sowie aktuelle Fragen des Datenschutzes präsentieren. Darüber hinaus wirkte ein Vertreter der DSA als Redner an der digma-Tagung zum Datenschutz in der täglichen Praxis von Städten und Gemeinden sowie an einem Online-Event der Fachagentur für ICT und Bildung (Educa) mit.

## 6.3 Formelle Stellungnahmen

### Änderung des Gesundheitsgesetzes

Erlasse und andere Massnahmen, welche für den Datenschutz erheblich sind, sind der DSA vorgängig zur Stellungnahme vorzulegen. Im Zentrum der Prüfung einer Änderung des Gesundheitsgesetzes (GesG) stand die Inspektion ambulanter Gesundheitsbetriebe. Im Rahmen einer solchen Inspektion soll neu Einsicht in besonders schützenswerte Personendaten (z.B. Behandlungsdokumentation) genommen werden können. Gleichzeitig sollen die für die Führung von ambulanten Gesundheitsbetrieben verantwortlichen Personen und die im Gesundheitsbetrieb mitwirkenden Personen zur umfassenden Mitwirkung verpflichtet werden. Dank eines konstruktiven Austausches zwischen der DSA und der federführenden Gesundheits- und Integrationsdirektion (GSI) konnte für die betreffende Vorschrift eine datenschutzrechtlich optimale Lösung gefunden werden. Hierbei mussten die jeweiligen Anforderungen des kantonalen Datenschutzes (für Datenbearbeitungen durch die kantonale Behörde), des Datenschutzgesetzes des Bundes (Datenbearbeitung durch Private) und des Strafgesetzbuches (Berufsgeheimnis) berücksichtigt werden.

Die gute Zusammenarbeit zwischen der DSA und der GSI führte auch bei weiteren Gesetzesvorhaben zu einer tragfähigen datenschutzrechtlichen Lösung, so namentlich beim neuen Gesetz über die Leistungen für Menschen mit Behinderung (BLG).

## Elektronisches Baubewilligungsverfahren

Mit einer Änderung des Baugesetzes und des Baubewilligungsdekrets sollen die Grundlagen für eine elektronische Durchführung des Baubewilligungsverfahrens geschaffen werden. Dabei ist vorgesehen, dass auch die Baugesuchsunterlagen während der öffentlichen Auflage in elektronischer Form zugänglich gemacht werden. Diese Unterlagen können besonders schützenswerte Angaben über den/die Gesuchsteller*in enthalten, etwa wenn es um den Einbau eines Behindertenaufzugs geht. Mit der bisherigen Auflage bei der Gemeindeverwaltung wird die Einsichtsmöglichkeit faktisch auf jene Dritten beschränkt, welche den Aufwand dazu auf sich zu nehmen bereit sind. Demgegenüber ist ein Zugang über das Internet grundsätzlich weltweit und mit automatisierten Mitteln möglich. Die DSA verlangte deshalb eine Vorschrift, wonach die Gemeinden angemessene Massnahmen zur Wahrung der Informationssicherheit und des Datenschutzes treffen müssen. Denkbar ist der Schutz des Zugangs mit einem nur für das betreffende Verfahren geltenden Passwort, welches während der Auflagedauer auf Anfrage bekannt gegeben wird. Siehe zur Prüfung der Fachanwendung «eBau» unten Ziff. 6.5.

## Ausführungsverordnungen zum PDSG

Das neue Gesetz über die zentralen Personendatensammlungen (PDSG) und die darauf gestützten Verordnungen konkretisieren das Prinzip «Once Only», wonach Personendaten, welche von mehreren Behörden zur Erfüllung ihrer jeweiligen Aufgaben benötigt werden (und gesetzlich bearbeitet werden dürfen), im Interesse der Richtigkeit und Vollständigkeit der Daten an einem zentralen Ort zum Abruf bereitgestellt werden. Eine Mitarbeiterin der DSA wirkte in der Arbeitsgruppe, welche die Verordnung über die Gemeinderegistersysteme-Plattform GERES (GERES V) und die Verordnung über die von der Steuerverwaltung betriebene Zentrale Personenverwaltung (ZPV V) vorbereitete, aktiv mit. Die neuen Erlasse treten am 1. März 2021 in Kraft und lösen das Gesetz sowie die Verordnung über die Harmonisierung amtlicher Register ab. Die neuen Verordnungen legen für den Zugang zu den Daten jeweils ein Basisprofil und für besondere Bedürfnisse gebildete Standardprofile fest. Für die DSA war wichtig, dass das Basisprofil, das grundsätzlich allen berechtigten Behörden zur Verfügung steht, keine besonders schützenswerten oder sonst sensiblen Daten enthält. Bei den Standardprofilen war sicherzustellen, dass nur ein aufgabenbezogener und verhältnismässiger Zugriff auf Personendaten ermöglicht wird. Dies führte dazu, dass etwa die Konfession oder die AHV-Nummer je ein eigenes Profil mit einer einzigen Angabe bilden. Die Direktionen werden die Berechtigungen der ihnen angehörenden oder zugeordneten Behörden in Direktionsverordnungen – welche der DSA vorgängig zur Stellungnahme zu unterbreiten sind – festlegen, für die Gemeindebehörden sind die Profile für den Zugang zu GERES direkt im Anhang zur Verordnung festgelegt.

## Gesetz über die digitale Verwaltung

Ein neues Gesetz über die digitale Verwaltung (DVG) soll die Grundsätze der Digitalisierung der öffentlichen Verwaltung im Kanton regeln. Die DSA hatte von Anfang an die Möglichkeit, in einer Begleitgruppe am Gesetzesentwurf mitzuarbeiten, wobei ihr Fokus klar auf den datenschutzrechtlichen Bestimmungen lag. Es erwies sich als nötig, für die vielfältigen digitalen Datenbearbeitungen Lücken im Datenschutzrecht zu schliessen und wichtige Verbesserungen vorzunehmen wie klare Regelungen zur Datenbearbeitung durch Dritte (Auftragsdatenbearbeitung), zur Datenschutzverantwortung, wenn mehrere Behörden über den Zweck und die Mittel einer Datenbearbeitung entscheiden, und zur Abstimmung der Aufsichtstätigkeit, wenn in behördenübergreifenden Vorhaben mehrere Datenschutzaufsichtsstellen mit der gleichen digitalen Datenbearbeitung befasst sind.

Diese Bestimmungen ergänzen das kantonale Datenschutzgesetz (KDSG) vorübergehend und werden im Rahmen der Revision des KDSG, die durch die neuen europäischen Datenschutzerlasse ausgelöst wurde, berücksichtigt werden.

## Bericht zum Einsatz von Bodycams bei der Kantonspolizei

Am 2. Dezember 2020 verabschiedete der Regierungsrat den Bericht «Einsatz von Körperkameras (Bodycams) bei der Kantonspolizei» in Erfüllung eines parlamentarischen Postulats. Er stellte darin in Aussicht, dass die Kantonspolizei ab 2021 vermehrt Bodycams einsetzen werde, soweit es die geltenden Rechtsgrundlagen erlauben. Das bernische Polizeigesetz und die schweizerische Strafprozessordnung lassen (auch verdeckte) Bildaufzeichnungen zu, wenn ernsthafte Anzeichen für eine bevorstehende Straftat bestehen bzw. eine solche begangen wurde und die Informationsbeschaffung sonst aussichtslos wäre oder unverhältnismässig erschwert würde. Zudem enthält das Polizeigesetz eine Grundlage für Videoüberwachungen bei Massenveranstaltungen, ohne sich zur Einsatzform – festinstalliert oder mobil – zu äussern. Die DSA nahm vor der Verabschiedung zum Bericht Stellung.

Videoüberwachungen benötigen grundsätzlich eine hohe demokratische Legitimation, weil sie nebst Tatverdächtigen oder Störern immer auch unbeteiligte Personen betreffen. Bei mobilen Kameras kommt dazu, dass sich Unbeteiligte nicht ohne weiteres aus dem Aufnahmefeld begeben können, weshalb ihr Einsatz im formellen Gesetz ausdrücklich vorgesehen werden sollte. Ist dies nicht der Fall, darf erwartet werden, dass mindestens die Regierung den Einsatz formell erlaubt und mittels Verordnung die nötige Transparenz schafft. Für Drohnen ist dies beim Erlass der neuen Polizeiverordnung per 1. Januar 2020 geschehen, mobile Bodycams sind jedoch nach wie vor nicht gesetzlich verankert.

# 6.4 Vorabkontrollen

## 6.4.1 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 123 Vorabkontrollen und Voranfragen (Vorjahr: 113) zu Informatikprojekten bearbeitet und dabei 58 (69) bzw. 47.2 % (61.1) der Vorabkontrollen 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.

### «Hospitalisation»

Bei der zur Vorabkontrolle unterbreiteten Applikation «Hospitalisation» (HOSP) handelt es sich um ein Instrument zur elektronischen Abwicklung von Spitalrechnungen und Kostengutsprachen für auswärtige Spitalbehandlungen. Sie steht als Beispiel für die fortschreitende Digitalisierung im Gesundheitsbereich, welche die Beteiligten auf allen Seiten vor anspruchsvolle rechtliche und technische Fragen stellt. Im vorliegenden Fall galt besondere Aufmerksamkeit der technischen Umsetzung von Datenabrufen von der Gemeinderegistersysteme-Plattform GERES, welche nicht durch einzelne Mitarbeitende, sondern durch ein System erfolgen sollen («Machine-to-Machine»-Anbindung). Eine solche Lösung führt regelmässig zu erhöhter Komplexität im Bereich der Berechtigungsverwaltung innerhalb der Applikation.

### Neue Fachapplikation Migration

Im Kanton Bern wurde der Asyl- und Flüchtlingsbereich per 1. Juli 2020 neu strukturiert und auf neue rechtliche Grundlagen gestellt. Die Anpassung hatte auch für die in diesem Bereich verwendeten Informatiksysteme eine Konsolidierung zur Folge. Die Neue Fachapplikation Migration (NFAM) löste eine Vielzahl von unterschiedlichen Applikationen ab, welche zuvor von den mit dem Vollzug

betrauten externen Stellen verwendet wurden. Die DSA wurde im Rahmen dieses sehr komplexen IT-Projekts früh begrüsst und tauschte sich mit der Projektleitung regelmässig und intensiv aus. Durch dieses in der Projektplanung berücksichtigte iterative Vorgehen konnte die DSA bei den zuständigen Behörden der Gesundheits- und Integrationsdirektion (GSI) sowie der Sicherheitsdirektion (SID) das Verständnis für den Datenschutz und die Informationssicherheit wecken, und die Behörden hatten trotz der Grösse des Vorhabens eine hohe Planungssicherheit, so dass die entsprechenden Meilensteine fristgerecht erreicht werden konnten.

## Neue Vorgangsbearbeitung «Rialto» der Kantonspolizei

Eine bedeutende Vorabkontrolle des Berichtsjahrs betraf die Neue Vorgangsbearbeitung (NeVo) «Rialto» der Kantonspolizei (KAPO). Damit soll die bisherige Systemlandschaft für die polizeiliche Vorgangsbearbeitung abgelöst und auf der Grundlage der Standardlösung SAP ICM (Investigative Case Management) realisiert werden. Mitbeteiligt ist auch die Staatsanwaltschaft des Kantons Bern (inkl. Jugendanwaltschaft), deren Daten aber auf einem strikt getrennten Mandanten bearbeitet werden. Angesichts der Grösse und der Komplexität des Vorhabens ergab eine erste Prüfung der DSA insgesamt 86 Befunde von mehrheitlich mittlerer Wesentlichkeit, welche sehr unterschiedliche Aspekte – vom Betriebsvertrag mit der Swisscom über die zulässigen Aufbewahrungsfristen bis hin zu technischen Massnahmen zur Gewährleistung der Datensicherheit – betrafen. Nach einer ausführlichen Stellungnahme der KAPO und einer Überarbeitung des Informationssicherheits- und Datenschutz (ISDS)-Konzepts verblieben nunmehr 10 Befunde, wobei ein neuer Punkt den Datenaustausch zwischen KAPO und Staatsanwaltschaft betraf. Nach deren Bereinigung – im Sinne, dass die KAPO die erforderlichen Massnahmen beschrieb und deren Umsetzung in Aussicht stellte – konnte die Vorabkontrolle schliesslich abgeschlossen werden.

In einem für den Datenschutz zentralen Punkt wird NeVo Rialto eine wesentliche Verbesserung bringen: Zur Gewährleistung ihrer Einsatzfähigkeit haben die Mitarbeitenden der KAPO teils weitreichende Einsichtsrechte in die in den Informationssystemen enthaltenen Daten, ohne dass reine Lesezugriffe protokolliert würden. Weil die Mitarbeitenden aber nur dann auf die teils hochsensiblen Daten zugreifen dürfen, wenn sie es zur Aufgabenerfüllung zwingend benötigen, sind geeignete Kontrollmechanismen erforderlich. In NeVo Rialto werden künftig auch Lesezugriffe protokolliert und mittels Stichproben überprüft.

## Anbindung «Dr. Tax» an das Gesamtsystem NESKO

Im Zuge der Digitalisierung beschloss die kantonale Steuerverwaltung, das elektronische Einreichen von Steuererklärungen zu ermöglichen, welche mit Hilfe von Drittsystemen ausgefüllt wurden. Bereits heute werden rund 100 000 Steuererklärungen mit der Software «Dr. Tax» ausgefüllt. Deshalb soll «Dr. Tax»

als erstes Drittsystem an das Gesamtsystem Neues Steuerkonzept (NESKO) der Steuerverwaltung angebunden werden. Die DSA prüfte den dafür nötigen neuen Online-Importservice, wobei diverse Aspekte der sicheren Übertragung der Daten zu klären waren.

**«GELAN Cloud»**

Der Kanton Bern betreibt die Gesamtlösung EDV Landwirtschaft und Natur (GELAN) für sich und gestützt auf entsprechende Leistungsvereinbarungen für die Kantone Freiburg und Solothurn. Im Rahmen einer Weiterentwicklung sollte GELAN als Cloud Service (Plattform as a Service) im Rechenzentrum der Bedag Informatik AG betrieben werden. Als wesentliche Änderung einer bestehenden Datenbearbeitung waren die Neuerungen der DSA zur Vorabkontrolle zu unterbreiten. Die DSA prüfte sowohl die geplante Migration der physikalischen Server des GELAN 4 in den neuen Cloud Service als auch den künftigen Betrieb durch die Bedag AG. Zu klären waren namentlich der Fernzugang mittels VPN (Virtual Private Network) sowie die Einhaltung der seit Januar 2020 geltenden Vorschriften der Randdatenverordnung (RDV).

**Immobiliendienstleistungen**

Die Standortförderung Kanton Bern (SFBE) bietet den Unternehmen eine Immobilienvermittlungsdienstleitung an. Mit der neuen Webapplikation «SFBE Immobiliendienstleistung» werden aktuelle Immobilien-Angebote künftig einheitlich aufbereitet und Anfragen standardisiert bearbeitet. Da Geschäftsgeheimnisse der Kunden betroffen sein können, welche einen erhöhten Schutzbedarf aufweisen, prüfte die DSA namentlich die Informationssicherheit der Anwendung, wobei sich betreffend die Benutzerkonten Fragen der Zugriffsberechtigungen und der Löschung inaktiver Accounts stellten.

### 6.4.2 Videoüberwachungen

Am 1. Januar 2020 trat das totalrevidierte Polizeigesetz (PolG) mit teilweise neuen Bestimmungen zu Videoüberwachungen in Kraft. Während die materiellen Anforderungen an Videoüberwachungen weitgehend unverändert aus dem früheren Recht übernommen wurden, ist für Überwachungen zum Schutz öffentlicher Gebäude neu keine Zustimmung der Kantonspolizei (KAPO) mehr nötig. Diese ist jedoch weiterhin in einem Rücksprachеverfahren zu konsultieren, wobei die KAPO das Ergebnis der Vorabkontolle der zuständigen Datenschutzaufsichtsstelle – für kantonale Behörden die DSA – berücksichtigt. Betreffend die Anforderungen an die Informationssicherheit und den Datenschutz (ISDS) erarbeitete die DSA eine ISDS-Checkliste, welche die KAPO auf ihrer Webseite als Hilfsmittel zur Verfügung stellt.

## Regionalgefängnis Thun und Justizvollzugsanstalt St. Johannsen

Die Videoüberwachungen in den Regionalgefängnissen und Strafvollzugsanstalten des Kantons Bern waren letztmals im Jahr 2010 von der DSA vorabkontrolliert worden. Seither haben sich die Technologie und die vorhandenen Installationen sowie auch die rechtlichen Grundlagen weiterentwickelt. Nebst den nach Polizeigesetz erlaubten Videoüberwachungen zur Verhinderung und Verfolgung von Straftaten sieht das Justizvollzugsgesetz von 2018 zusätzlich vor, dass Videoaufnahmen zur Unterstützung der Aufgabenerfüllung im Strafvollzug (wie zur Überwachung des Gesundheitszustands von Eingewiesenen) erstellt werden dürfen. Deshalb sahen die DSA und das zuständige Amt für Justizvollzug (AJV) vor, dass die ISDS-Unterlagen für sämtliche Institutionen aktualisiert und erneut von der DSA geprüft werden. Nach Eingang einer Bürgerbeschwerde wurde als erste Institution das Regionalgefängnis Thun geprüft, wobei auch eine Begehung vor Ort stattfand. Dabei ergab sich, dass die Überwachung grundsätzlich gesetzeskonform war, wobei gleichwohl punktuelle Anpassungen – namentlich die Korrektur des Bildausschnittes von Aussenkameras sowie der Umgang mit Kameras, deren Ausrichtung und Zoom vom diensthabenden Personal verändert werden konnte – erforderlich waren. Eine zweite Begehung betraf die Justizvollzugsanstalt St. Johannsen, welche als offene Vollzugseinrichtung andere Bedürfnisse aufweist als ein Gefängnis.

## Institut für Infektionskrankheiten

Das Institut für Infektionskrankheiten (ifik) der medizinischen Fakultät der Universität Bern verfügt über ein Biosicherheitslabor der Stufe 3. Dieses Labor ist nach den Vorgaben der Einschliessungsverordnung des Bundes (ESV) zu schützen. Die Videoüberwachung gilt als eine der geeignetsten Massnahmen. Das Institut reichte deshalb nach einer Vorbesprechung die nötigen Unterlagen für die Vorabkontrolle ein. Die DSA prüfte die geplante Überwachung mit sechs Kameras. Die Prüfung umfasste insbesondere Aspekte der Verhältnismässigkeit und der Datensicherheit.

Die Vorabkontrolle führte auch zur Klärung einer Frage zur Vernichtung von Videoaufzeichnungen. Die DSA war der Ansicht, dass Hausrechtsinhaber Aufzeichnungen, welche sie aufgrund eines Vorfalls an die Kantonspolizei (KAPO) übermitteln, unmittelbar danach auf ihrem Speichermedium vernichten müssen. Im Rahmen der vorliegenden Vorabkontrolle bestätigte die KAPO die Auffassung der DSA.

# 6.5 Audits

Im Berichtsjahr führte die DSA insgesamt sieben Informationssicherheits- und Datenschutzprüfungen (ISDS-Prüfungen) durch, wovon fünf in Zusammenarbeit mit einem qualifizierten Partner. Eine Prüfung konnte noch nicht abgeschlossen werden. Bei zehn abgeschlossenen ISDS-Prüfungen aus den Jahren 2016 – 2019 begleitete die DSA die kontinuierliche Umsetzung von Verbesserungsmassnahmen aktiv, wobei ein Geschäft erfolgreich abgeschlossen werden konnte.

Bei der Begleitung der Folgearbeiten zu den ISDS-Prüfungen der Vorjahre 2016 – 2019 stellte die DSA fest, dass eine langfristige Umsetzung von formellen, technischen oder organisatorischen ISDS-Verbesserungsmassnahmen eine konsequent hohe Aufmerksamkeit von den verantwortlichen Stellen fordert, welche aus Sicht der DSA nicht immer im gewünschten Masse vorhanden war. Es entstand teilweise ein erheblicher Aufgabenrückstau. Die Gründe dazu finden sich unter anderem im herausfordernden Tagesgeschäft und bei den im Berichtsjahr herrschenden ausserordentlichen Rahmenbedingungen aufgrund der behördlichen Massnahmen zur Eindämmung der Pandemie. Je länger die Umsetzung von ISDS-Verbesserungsmassnahmen dauert, desto grösser wird das Risiko, dass der sich laufend ändernden Bedrohungslage im Bereich der Cybersicherheit nicht gerecht werden kann. Die DSA erwartet daher, dass die verantwortlichen Stellen und Entscheidträger jenes Risiko bei der Priorisierung der Aufgaben mitberücksichtigen.

**Active Directory (AD) Services / Management**

Prüfgebiet: Die Prüfung umfasste den zentralen Verzeichnisdienst Microsoft Active Directory (AD) beim Amt für Informatik und Organisation des Kantons Bern (KAIO). Das KAIO stellt die AD-Dienste für die kantonale Verwaltung zur Verfügung. Die AD-Dienste werden über sog. Domain-Controller und -Server bereitgestellt, welche von der Bedag Informatik AG betrieben und verwaltet werden. Mit den AD-Diensten wird das technische Netzwerk entsprechend der organisatorischen Struktur der kantonalen Verwaltung gegliedert. Die AD-Dienste verwalten dabei verschiedene Objekte im kantonalen Netzwerk, wie beispielsweise die erfassten Benutzer, Gruppen, Computer, weitere Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner mit deren eindeutigen Eigenschaften. Ein System-Administrator kann die Informationen zu den erfassten Objekten organisieren, bereitstellen und überwachen.

Prüfziel: Dieses umfasste die Beurteilung der AD-Sicherheit mit den Umsystemen, Schnittstellen sowie dem AD-Change und Release-Management (CRM), das AD-Konfigurations-Management, Kontroll- und QS-Massnahmen, Zugriffsmanagement, Datenhaltung und Support.

Prüfergebnis: Das Gesamtergebnis der Prüfung wies in allen Prüfbereichen Befunde mit hohen und mittleren Risiken und entsprechend ein substanzielles Verbesserungs- und Optimierungspotential aus. Generell wurde die in einer nicht aktuellen Version vorliegende konzeptionelle AD-Dokumentation bemängelt. Es fehlte dadurch eine verbindliche SOLL-Vorgabe für den AD-Betrieb. Insbesondere die Handhabung von privilegierten und damit hohen Zugriffsrechte bedarf einer besseren konzeptionellen Darstellung und weitergehenden Zugriffseinschränkungen. Das konsequente Durchsetzen und Kontrollieren der Wirksamkeit von Passwortrichtlinien und das Schwachstellenmanagement muss ebenfalls weiter verbessert werden.

Die Zusammenarbeit erfolgte in einem professionellen und kooperativen Umfeld. Die DSA wird die Umsetzung der Verbesserungsmassnahmen aktiv begleiten.

## BE-Login

Prüfgebiet: BE-Login ist das Anmelde-Portal für E-Government-Angebote, welche den Bürger*innen und den Mitarbeitenden der kantonalen Stellen den Zugang zu den enthaltenen Fachapplikationen der kantonalen Verwaltung ermöglicht. BE-Login wird durch das Amt für Informatik und Organisation des Kantons Bern (KAIO) verantwortet sowie durch die Bedag Informatik AG entwickelt und betrieben.

Prüfziel: Dieses umfasste die Beurteilung der Informationssicherheit von BE-Login mittels Code-Inspektion gemäss dem *Open Web Application Security Project* (OWASP), der Sicherheit mit den Umsystemen, Schnittstellen, Change und Release-Management (CRM) und Konfigurations-Management, Kontroll- und QS-Massnahmen, Zugriffsmanagement, User-Login, Datenhaltung und Support.

Prüfergebnis: Im Rahmen der Prüfung wurden in den Prüfbereichen «Sicherer Software Code», Login-Prozess und Betriebsprozesse Befunde mit teils hohen Risiken festgestellt. Hier erwartete die DSA unmittelbar Verbesserungsmassnahmen. Zudem stellte sie weitere Befunde mit mittlerem und tiefem Risiko fest. Insgesamt wies BE-Login im Zeitpunkt der Prüfungshandlungen erhebliche Sicherheitsmängel auf. Da im Zuge der Digitalisierung der kantonalen Verwaltung weitere Applikationen an BE-Login angeschlossen werden, wird sich die Exponiertheit des Portals weiter erhöhen. Die DSA äusserte deshalb die Erwartung, dass die Mängel entsprechend ihrer Kritikalität zeitnah angegangen werden, um das Sicherheitsniveau aller angeschlossenen Applikationen rasch zu erhöhen. Sie empfahl weiter, dass bis zur nachweisbaren Behebung der kritischen Befunde keine weiteren Applikationen an BE-Login anzubinden sind. Das KAIO folgte dieser Empfehlung im Grundsatz.

Die Zusammenarbeit erfolgte in einem professionellen und kooperativen Umfeld. Die DSA wird die Umsetzung der Verbesserungsmassnahmen aktiv begleiten und behält sich eine weitergehende Prüfung der Umsetzungsmassnahmen vor.

## ICT-Grundschutz bei der BFH

Prüfgebiet: Die Berner Fachhochschule (BFH) zählt etwa 7 000 Studierende und 2 500 Mitarbeitende. Sie hat heute 26 Standorte in Bern, Biel, Burgdorf, Magglingen, Nidau, Vauffelin und Zollikofen. Im Bereich der Informations- und Kommunikationstechnologie (ICT) werden zentrale Dienstleistungen von der Abteilung IT-Services erbracht. Zusätzlich betreiben die Departemente eigene ICT-Umgebungen, beispielsweise bei der Wirtschaftsinformatik bzw. für Laborbetriebe; diese Bereiche werden nicht von der Abteilung IT-Services verantwortet. Die ICT-Umgebung der BFH ist autonom von derjenigen der kantonalen Verwaltung. Einzelne Anwendungen der kantonalen Verwaltung – insbesondere im Personalbereich – werden verwendet.

Prüfziel: Es wurde geprüft, inwiefern die Anforderungen an die Informationssicherheit und den Datenschutz (ISDS) durch den ICT-Grundschutz und durch die implementierten ISDS-Massnahmen erfüllt werden. Im Rahmen dieser Prüfung wurden Dokumente gesichtet, Interviews mit den verantwortlichen Personen der Abteilung IT-Services geführt sowie punktuell technische Tests und Inspektionen von technischen Systemen durchgeführt.

Prüfergebnis: Im Rahmen der vollzogenen Prüfung wurden über alle Prüfbereiche hinweg Befunde mit einem mittleren, aber auch mit einem hohen Risiko festgestellt. Der BFH ICT-Grundschutz kann zum Zeitpunkt der Prüfungshandlungen noch nicht als angemessen qualifiziert werden. Mit dem gestarteten BFH-Projekt Informationssicherheits-Management-System (BFH ISMS) soll die Grundlage für einen angemessenen und aktiv gesteuerten ICT-Grundschutz gelegt werden.

Die Zusammenarbeit erfolgte in einem professionellen und kooperativen Umfeld. Die DSA wird das laufende BFH ISMS-Projekt und die Ergebnisse zu gegebenem Zeitpunkt erneut beurteilen.

## Fachanwendung eBau

Prüfgebiet: Im 2014 wurde die eingereichte Motion zur «Vereinfachung des Baubewilligungsverfahrens» durch den Grossrat des Kantons Bern bewilligt. Mit der Umsetzung des zum Zeitpunkt der Prüfungshandlungen von 2015 bis 2022 laufenden eBau-Projektes soll das Baubewilligungsverfahren im Kanton Bern flächendeckend digitalisiert werden. Die auf Web-Technologie basierende eBau-Lösung wird nach Abschluss des Projekts verbindlich eingesetzt werden. Die Lösung deckt dabei den gesamten Prozess des Baubewilligungsverfahrens vom Gesuchsteller über die Baubewilligungsbehörde bis zur Prüfung über die Amts- und Fachstellen ab.

Prüfziel: Die Prüfungshandlungen umfassten die Prüfgebiete ISDS-Governance, ISDS-Konzepte und Schutzmassnahmen, die Prozesse des Benutzermanagements, das Outsourcing und die Datenhaltung sowie Schnittstellen. Im Rahmen der

Prüfung wurden Dokumente gesichtet und Interviews mit den verantwortlichen Personen geführt.

Prüfergebnis: Die Prüfungshandlungen wurden im 2020 noch nicht abgeschlossen. Die DSA konnte nicht alle notwendigen Dokumente und Nachweise prüfen, da diese zum Zeitpunkt der Prüfungshandlungen teilweise nicht oder nicht in einer aktuellen Version zur Verfügung gestellt wurden. Die DSA wird die Prüfung im Jahr 2021 abschliessen können.

## BE-GEVER Basissystem

Prüfgebiet: Das Geschäftsverwaltungssystem resp. der kantonale Service BE-GEVER unterstützt mit der Lösung CMI AXIOMA der Firma CM Informatik AG die Funktionalitäten einer verwaltungsweiten Gesamtlösung für die Geschäfts- und Dokumentenverwaltung und Aktenführung, Ablaufsteuerung sowie Geschäftskontrolle. Die geschäftsrelevanten Dokumente der kantonalen Verwaltung müssen weisungsbasiert mit dem Service BE-GEVER bzw. dem Geschäftsverwaltungssystem verwaltet werden. Der BE-GEVER Service mit dem Basissystem wird durch das Amt für Informatik und Organisation (KAIO) verantwortet und durch die Bedag Informatik AG betrieben. BE-GEVER erlaubt es den Direktionen und der Staatskanzlei bzw. kantonalen Ämtern, mittels dedizierter Mandanten in eigenen logischen Umgebungen zu arbeiten. Die Dokumentenarchivierung ist hierbei nicht Teil von BE-GEVER.

Prüfziel: Die Prüfung umfasste die bestehenden Anforderungen an die Informationssicherheit und den Datenschutz (ISDS) beim kantonalen Geschäftsverwaltungsbasissystem BE-GEVER. Im Rahmen der Prüfung wurden Dokumente und das BE-GEVER Basissystem gesichtet sowie Interviews mit den verantwortlichen Personen des KAIO und der Bedag Informatik AG geführt.

Prüfergebnis: Über alle Prüfbereiche hinweg wurden Befunde gemacht, welche zum grossen Teil mit einem mittleren, teilweise aber auch mit einem hohen Risiko eingestuft wurden. Insbesondere lag kein aktuelles und vollständiges ISDS-Konzept für den realisierten Betrieb vor. Weiter wurde festgestellt, dass die in BE-GEVER verwalteten Dokumente auf Datei-Servern (File-Ablagen) und nicht in einer dezidierten Datenbank gespeichert werden. Unautorisierte und unerkannte Lesezugriffe auf Dokumente auf den Datei-Servern (z. B. mit erhöhten Rechten als System-Administrator) können dabei nicht ausgeschlossen werden. Die DSA gelangte deshalb zur Beurteilung, dass zum Zeitpunkt der Prüfungshandlungen die Vertraulichkeit der Personendaten und anderen schutzwürdigen Informationen in allen Mandanten von BE-GEVER nicht vollständig und transparent gewährleistet war. Sie äusserte die Erwartung, dass die notwendigen Massnahmen zur nachweisbaren Sicherstellung der Vertraulichkeit der in BE-GEVER bearbeiteten Daten rasch umgesetzt werden. Weiter empfahl die DSA, dass als «geheim» eingestufte Dokumente und Daten nicht in BE-GEVER bearbeitet werden sollten.

Die Zusammenarbeit erfolgte in einem professionellen und kooperativen Umfeld. Die DSA wird die Umsetzung der Verbesserungsmassnahmen aktiv begleiten und behält sich eine Nachprüfung der Umsetzungsmassnahmen vor.

## ICT-Grundschutz bei der Spital STS AG Thun

Prüfgebiet: Die Spital Simmental-Thun-Saanenland AG (Spital STS AG) zählt über 1 900 teil- und vollzeitangestellte Mitarbeitende. Das Spital Thun ist verantwortlich für die medizinische Spitalversorgung (Grundversorgung und spezialisierte Leistungen) sowie ein interdisziplinäres Notfallzentrum. Alle für den Spitalbetrieb nötigen Fachbereiche wie Facility Management, ICT/Informatik, Verwaltung, Technik etc. sind am Standort Thun untergebracht. Weitere Unternehmen der Spital STS AG sind neben dem Spital Thun das Spital Zweisimmen, die Psychiatrischen Dienste und der Rettungsdienst. Die ICT-Organisation wird vom *Chief Information Officer* geführt und beinhaltet die Bereiche ICT Infrastruktur, Applikationen und Medizininformatik, welche jeweils von einer Leitung verantwortet werden. Zentrale ICT-Systeme sind in den Rechenzentrums-Räumen am Spital Thun untergebracht, andere Standorte haben grundsätzlich keine lokalen Server-Systeme und nutzen die zentralen Systeme am Spital Thun.

Prüfziel: Dieses umfasste die Beurteilung der nachweisbaren Erfüllung von Anforderungen an die Informationssicherheit und den Datenschutz (ISDS) durch den ICT-Grundschutz und die implementierten ISDS-Massnahmen. Insbesondere sollten die Themen ISDS-Governance, ISDS-Konzept, Change- und Release-Management, Zugriffsmanagement, Netzwerk-Sicherheit, Storage-Sicherheit, Client- und Server-Sicherheit, Outsourcing, Pendenzen aus der Prüfung von 2012 sowie die physische Sicherheit am Standort Thun beurteilt werden. Im Rahmen der Prüfung wurden Dokumente gesichtet, Interviews mit den verantwortlichen Personen geführt sowie punktuell technische Tests und Inspektionen durchgeführt.

Prüfergebnis: Im Rahmen der Prüfung wurden über alle Prüfbereiche hinweg Befunde gemacht, welche teils mit einem tiefen und teils mit einem mittel-hohen Risiko eingestuft wurden. Grundsätzlich bestehen gute Voraussetzungen für einen angemessenen ICT-Grundschutz. Dennoch sollten schon erkannte ISDS-Massnahmen und -Aufgaben klarer risikobasiert priorisiert und entsprechend terminiert umgesetzt sowie auf Wirksamkeit überprüft werden. Auch eine systematische Härtung und Überprüfung von technischen Systemen kann noch nicht vollständig erkannt werden. Weiter bestehen Verbesserungsmöglichkeiten bei der Sicherung des Datenverkehrs im und durch das Netzwerk.

Die Zusammenarbeit erfolgte in einem professionellen und kooperativen Umfeld. Die DSA wird die Umsetzung der Verbesserungsmassnahmen aktiv begleiten.

**Schengen-Informationssystem MIDI**

Prüfgebiet: Mit der Übernahme des Schengen-Acquis verpflichtete sich die Schweiz, die datenschutzkonforme Nutzung des Schengener Informationssystem (SIS) zu gewährleisten und periodisch zu prüfen. Letzteres ist im Kanton Bern die Aufgabe der DSA. Diese prüfte im Herbst 2020 die SIS-Zugriffe durch den Migrationsdienst des Kantons Bern (MIDI).

Prüfziel: Gegenstand der Schengen-Kontrolle ist die Einhaltung der rechtlichen Vorgaben bei der Nutzung des Schengener Informationssystems (SIS) und umfasste bei dieser Prüfung die SIS-Zugriffe, das Datenschutzbewusstsein der MIDI-Mitarbeitenden, das Berechtigungsmanagement, das Ergebnis der jährlichen SIS-Berechtigungskontrollen und eine Nachfrage zu MIDI-Rollen mit bestehenden SIS-Zugriffsberechtigungen.

Prüfergebnis: Bei den überprüften MIDI SIS-Zugriffen stellte die DSA fest, dass das SIS für die MIDI-Aufgaben konform genutzt wurde. So lagen keine offensichtlichen Unregelmässigkeiten wie Abfragen zur eigenen Person oder von Personen des öffentlichen Lebens vor. Jedoch konnte ein Defizit an regelmässiger SIS-Schulung und -Information festgestellt werden. Auch das Ergebnis einer regelmässigen Kontrolle der bestehenden SIS-Zugriffsrechte konnte nicht aufgezeigt werden. Weiter besteht keine konzeptionelle SOLL-Dokumentation zum bestehenden Berechtigungsmanagement. Die DSA empfahl dem MIDI die Behebung der aufgezeigten Mängel.

## 6.6 Weitere aufsichtsrechtliche Instrumente

### 6.6.1 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. 3–5 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.

### 6.6.2 Oberaufsicht über die Aufsichtsstellen der Gemeinden

#### Weiterentwicklung der kommunalen Datenschutzaufsicht

Im Berichtsjahr 2019 hatte die DSA festgestellt, dass die aktuellen rechtlichen und technischen Herausforderungen viele der kommunalen Datenschutzaufsichtsstellen an ihre Grenzen bringen und die Gemeinden oftmals nur ungenügend beraten sind (siehe Jahresbericht 2019, S. 31). Die angelaufene Revision des Datenschutzgesetzes (KDSG) bietet nun die Gelegenheit, die Vorschrift, dass jede Gemeinde für ihren Bereich eine eigene Aufsichtsstelle bezeichnen muss, zu überprüfen und ggf. anzupassen. Darum lud die DSA zunächst den Verein Bernische Gemeinden (VBG) und das Amt für Gemeinden und Raumordnung (AGR) dazu ein, in einer informellen Arbeitsgruppe den Handlungsbedarf zu bestätigen und mögliche Lösungen zu entwerfen. Das Ergebnis wurde anschliessend einem grösseren Kreis mit einer Vertretung der Regierungsstatthalter und sechs Gemeinden verschiedener Grösse vorgestellt, diskutiert und weiterentwickelt.

Als Stossrichtung zeichnet sich ab, dass die allermeisten Gemeinden von der Pflicht zur Führung einer eigenen Aufsichtsstelle entbunden werden sollen und stattdessen die Datenschutzberatung und -aufsicht durch die DSA als gesamtkantonales Kompetenzzentrum erfolgen soll. Nur noch die grössten Gemeinden mit komplexen IT-Systemen sollen über eine eigene Aufsichtsstelle verfügen, welche die örtlichen Verhältnisse kennt und im ständigen Austausch mit den verantwortlichen Behörden steht. Diese Arbeitshypothese erfordert eine vertiefte Auseinandersetzung mit dem Aufgabenkatalog der Aufsichtsstelle sowie eine Klärung des Verhältnisses zwischen der Datenschutzaufsicht und der gemeinderechtlichen Aufsicht durch die Regierungsstatthalter.

Das Ergebnis der Vorarbeiten wird die DSA im Auftrag der Arbeitsgruppe in die angelaufene KDSG-Revision einbringen. Die Vorschläge werden im Rahmen des normalen Gesetzgebungsverfahren, für das die Direktion für Inneres und Justiz (DIJ) federführend zuständig ist, öffentlich zur Diskussion gestellt werden.

#### Beratung zu kommunalen Videoüberwachungen

Mehrere Datenschutzaufsichtsstellen von Gemeinden traten mit der Bitte um Unterstützung bei der Beurteilung kommunaler Videoüberwachungen an öffentlichen Orten und zum Schutz kommunaler Gebäude an die DSA heran. Bei einem Gemeindeverband und einer Gemeinde ging es jeweils um Schulanlagen, beim Gemeindeverband sollte zusätzlich zu den Gebäuden ein Grillplatz auf

dem Schulareal überwacht werden. Die DSA stellte den Aufsichtsstellen Unterlagen für die Vorabkontrolle und den Bericht sowie eine Checkliste für die Prüfung der Informationssicherheit und des Datenschutzes zur Verfügung. Von der DSA beantwortete Rückfragen betrafen Aspekte der technischen Datensicherheit (z.B. für aufgezeichnete Bilder), der Verhältnismässigkeit (z.B. zum Fokus der Kameras) und der Rechtmässigkeit (z.B. zum Zugriff auf die Bilder ausschliesslich durch die Kantonspolizei).

### Beratung der Aufsichtsstellen der Landeskirchen

Mit Erlass des neuen Landeskirchengesetzes (LKG) erhielten die drei Landeskirchen die Zuständigkeit, je eigene Aufsichtsstellen zu bezeichnen. Die Aufsichtsstelle der evangelisch-reformierten Landeskirche wandte sich mit einer Frage an die DSA, bei der es um den Datenaustausch nach dem Konkordat betreffend die gemeinsame Ausbildung der evangelisch-reformierten Pfarrer*innen und ihre Zulassung zum Kirchendienst ging. Das Konkordat bezweckt den Austausch von Angaben über die Eignung, damit «Pfarrpersonen, die nur unzureichend oder gar nicht in der Lage sind, ein Pfarramt zu führen, nicht einfach die Kirchgemeinde oder Landeskirche wechseln können». Da die evangelisch-reformierte Landeskirche nicht Mitglied des Konkordats ist, wollte sie die Voraussetzungen klären, nach denen sie an diesem Austausch teilnehmen kann. Die Abklärung der DSA ergab, dass das LKG die Voraussetzungen für die Anstellung von Geistlichen regelt und festhält, dass das landeskirchliche Recht weitere Anstellungsvoraussetzungen festlegen kann. Angaben über die Eignung im Sinne des Konkordats gehören jedoch nicht dazu. Solche Angaben dürften in aller Regel besonders schützenswerte Personendaten sein, für deren Bearbeitung das Datenschutzgesetz eine klare Rechtsgrundlage verlangt (Art. 6 Bst. a KDSG). Da weder das LKG noch das landeskirchliche Recht über eine klare Regelung – auch nicht für den Datenaustausch mit Landeskirchen anderer Kantone – enthalten, kam die DSA zum Schluss, dass eine entsprechende Rechtsgrundlage dafür geschaffen werden oder die Landeskirche dem Konkordat beitreten müsste.

## 6.7 Interkantonale Zusammenarbeit

### Arbeitsgruppen von privatim

Die *Arbeitsgruppe Digitale Verwaltung* befasste sich ausführlich mit der neuen Pflicht der Behörden, den Datenschutzbehörden Datenschutzvorfälle zu melden. Im Kanton Bern gilt diese Pflicht seit dem 1. September 2018 für bestimmte Behörden der Polizei und Justiz (Art. 1 Abs. 1 Einführungsverordnung zur EU-Datenschutzrichtlinie). Die Arbeitsgruppe erarbeitete ein Muster-Meldeformular für

die Behörden und ein Prozesspapier für die Datenschutzbehörden, welche die Meldungen bearbeiten müssen. Die von privatim zur Verfügung gestellten Vorlagen wurde von der DSA an die Vorgaben des kantonalen Rechts angepasst. Das Meldeformular steht den Behörden auf der Webseite der DSA zum Abruf zur Verfügung.

Die *Arbeitsgruppe Sicherheit* unterzog Unterlagen des Vereins Electronic Monitoring zum Datenschutz einer fachlichen Review. Der Verein soll unter Beizug von externen Lieferanten eine Infrastruktur aufbauen, welche von den Kantonen für die Durchsetzung von Hausarresten, Rayon- oder Kontaktverboten mittels elektronischer «Fussfesseln» genutzt werden kann. Die Arbeitsgruppe zeigte auf, welcher Partei welche datenschutzrechtliche Rolle und Verantwortung zukommt, und wies auf eine Reihe von Anforderungen hin, die zu erfüllen sind, damit die Infrastruktur den datenschutzrechtlichen Vorschriften der Kantone entsprechen wird.

Die schon früher bestehende *Arbeitsgruppe Gesundheit* nahm ihre Arbeit im Berichtsjahr unter der Leitung der stellvertretenden Datenschutzbeauftragten der DSA wieder auf. Sie befasste sich hauptsächlich mit dem elektronischen Patientendossier und jeweils kurzfristig mit aktuellen datenschutzrechtlichen Fragen zur Corona-Pandemiebekämpfung (namentlich Internetpublikation anonymisierter Positivfälle sowie Datenerhebung und -speicherung beim Contact Tracing).

In der *Arbeitsgruppe ICT* tauschten sich Vertreter jener kantonalen Aufsichtsstellen, welche über eigene Informatiker verfügen, über aktuelle Fragen der Informationssicherheit aus.

### Swiss Library Service Platform (SLSP)

Für das neue gesamtschweizerische Bibliotheksverwaltungssystem SLSP, welches anfangs 2021 die bisherigen Hochschulbibliothekskataloge ablöst, wurde erstmals eine überkantonale Vorabkontrolle durchgeführt. Die Datenschutzaufsichtsstellen der Kantone Basel-Stadt, Zürich und Bern prüften die eingereichten ISDS-Unterlagen gemeinsam unter Berücksichtigung kantonalrechtlicher Unterschiede. So entstand eine einheitliche Beurteilung, auf welche sich auch die übrigen Kantone abstützen können.

### Krebsregister Bern Solothurn (KRBESO)

Das Krebsregister Bern Solothurn erfasst Tumordaten für den Kanton Bern seit 2013 und für den Kanton Solothurn seit 2019. Das Register wird mit einer neuen Registrierungssoftware geführt, welche die gesetzlichen Auflagen des am 1.1.2020 in Kraft getretenen Krebsregistrierungsgesetzes erfüllt. Die DSA verfasste einen ersten Prüfbericht, den sie zur Verwendung der Resultate und Erkenntnisse auch der Datenschutzaufsichtsstelle des Kantons Solothurn zustellte.

# 7 Antrag

Kenntnisnahme.

Datenschutzaufsichtsstelle
des Kantons Bern

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

www.be.ch/dsa