Kanton Bern
Canton de Berne

Jahresbericht Datenschutzaufsichtsstelle 2021

Datenschutzaufsichtsstelle

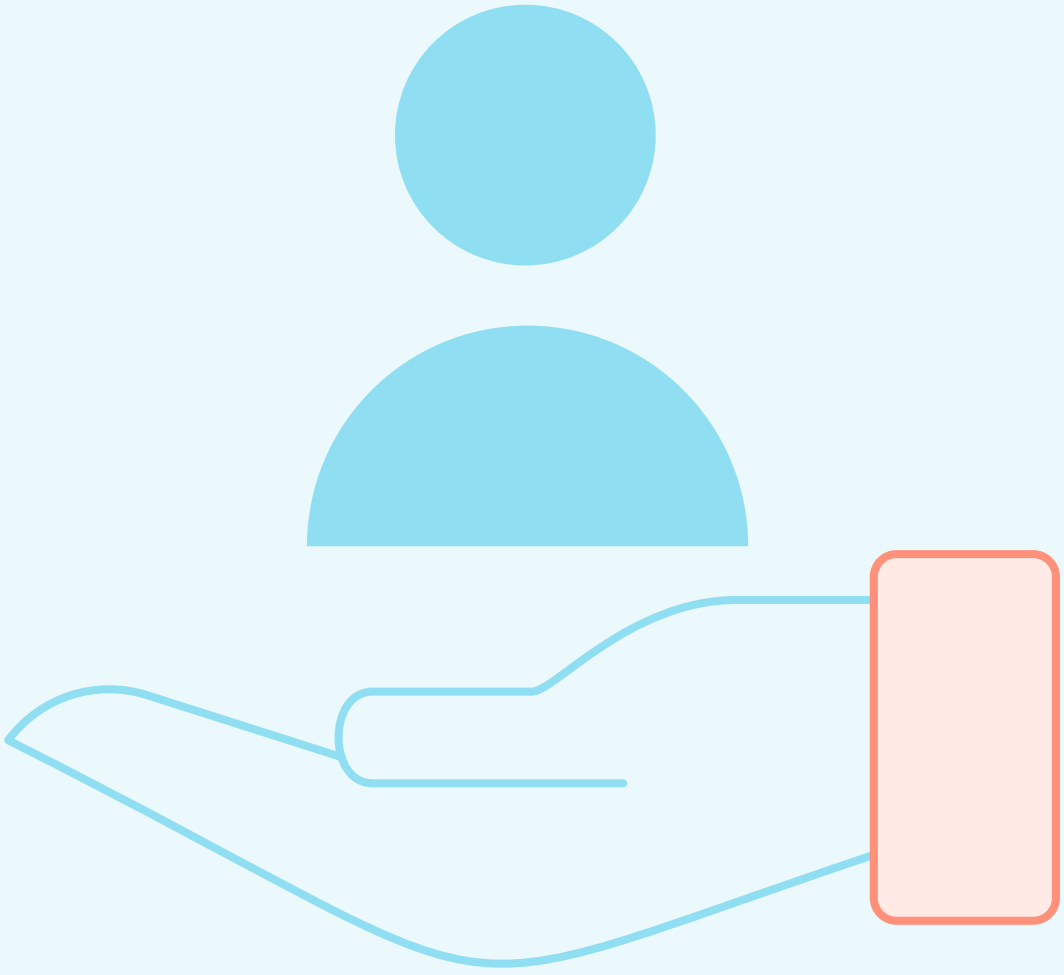
Februar 2022

Impressum

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

Layout und Realisation: noord.ch

Inhaltsverzeichnis



1 Vorwort

Es gehört zur Natur des Datenschutzrechts und ist dessen Kernaufgabe, mittels rechtsstaatlicher Regeln den «richtigen» Ausgleich zwischen privaten Grundrechten – hier auf Schutz der Privatsphäre – und öffentlichen Aufgaben herbeizuführen. Dabei macht es grundsätzlich keinen Unterschied, ob die öffentlichen Interessen einer allgemeinen Entwicklung wie der digitalen Transformation der Verwaltung oder einer besonderen Lage z. B. im Bereich der Gesundheit entspringen. Auch in einer Pandemie stehen sich der öfffentliche Auftrag und der Schutz der Privatsphäre nie im Sinne von «entweder/oder» gegenüber, vielmehr ist stets ein sachgerechtes «sowohl/als auch» zu finden. Dass dabei je nach Bedarf an Massnahmen zum Schutz der Gesundheit die Privatsphäre mehr oder weniger zurückgedrängt werden kann, gehört – solange die verfassungsrechtlichen Garantien eingehalten werden – zum Selbstverständnis des Datenschutzrechts.

Wenn der Datenschutz während der Pandemie gleichwohl besondere Herausforderungen erfährt, hat dies andere Gründe als das gewohnte Spannungsverhältnis zwischen privaten und öffentlichen Interessen: So erweist sich schon der Umgang mit der Grundanforderung, dass sich jede Datenbearbeitung auf eine hinreichende Rechtsgrundlage stützen muss, als schwierig, wenn sich die gesetzlichen Grundlagen ständig (und teils in verkürzten Rechtssetzungsprozessen) ändern, der Bund und die Kantone teils parallele Regelungskompetenzen aufweisen und sich zudem die Frage stellt, ob die vom Gesetzgeber an die Regierung delegierten Kompetenzen erlauben, dass diese vorübergehend Regelungen auf Verordnungsebene trifft, welche in «normalen» Zeiten aus rechtsstaatlicher Sicht in ein formelles Gesetz gehören würden. Auch die Beurteilung der Verhältnismässigkeit wird anspruchsvoller, wenn in der Gesellschaft schon Uneinigkeit über die Intensität der Bedrohung besteht, sich die Informationslage laufend weiterentwickelt und eine konkrete Datenbearbeitung (wie die Schaffung einer zentralen Kontaktdatenbank) regelmässig nicht als Einzelmassnahme, sondern als Bestandteil eines umfassenderen Massnahmenbündels verstanden wird.

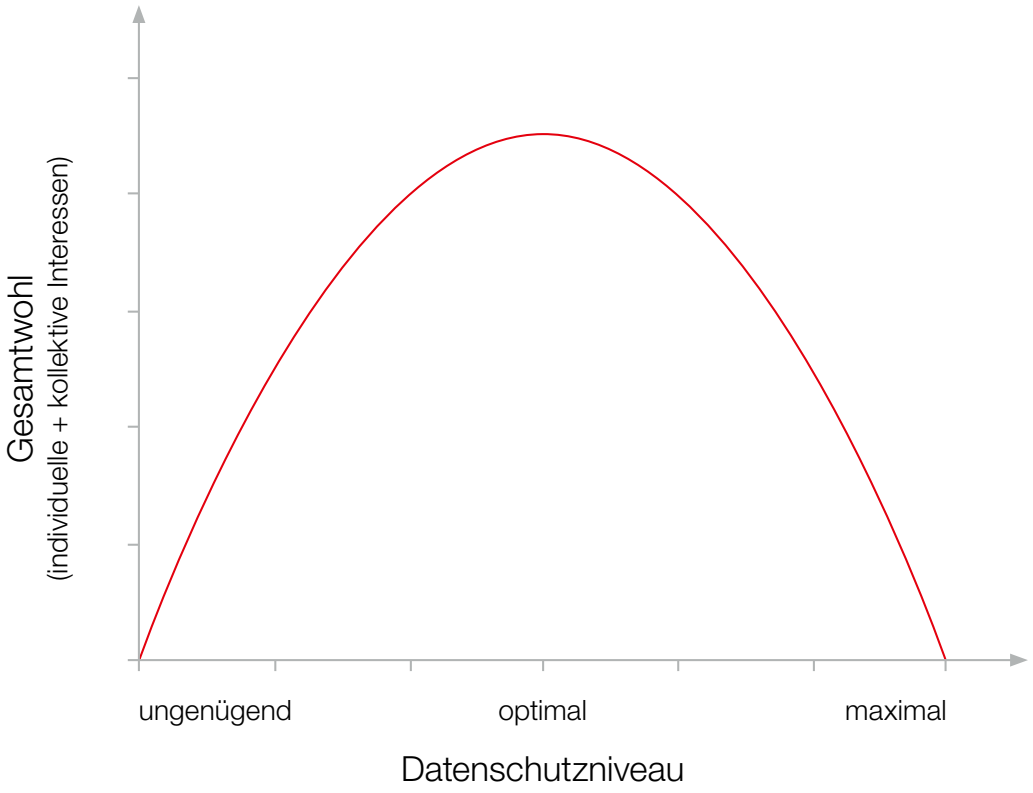
Vor diesem Hintergrund enthält der vorliegende Bericht erneut ein eigenes Kapitel über ausgewählte Geschäfte im Zusammenhang mit der Pandemie (Ziff. 6.1). Zudem erwies es sich einmal mehr als sehr wertvoll, dass die kantonalen Datenschutzbehörden unter sich und mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten einen engen Austausch pflegen, um die grossen datenschutzrechtlichen Herausforderungen – auch über die Pandemie hinaus – gemeinsam und aufeinander abgestimmt zu meistern (siehe dazu Ziff. 6.7).

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.



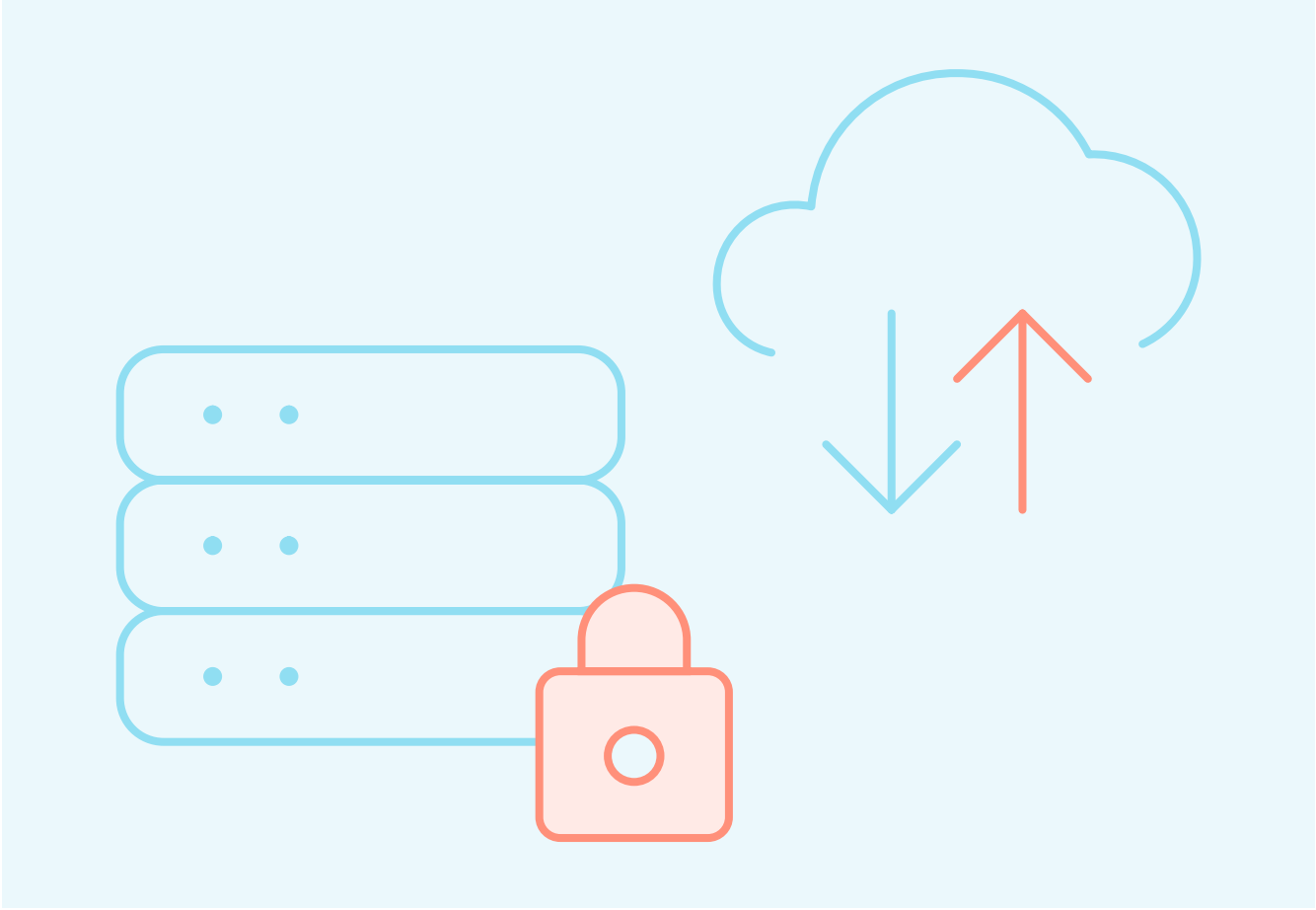
Das Datenschutzgesetz (KDSG) konkretisiert die Pflichten der Behörden beim Bearbeiten von Personendaten, wobei nebst der Verwaltung auch weitere Träger von öffentlichen Aufgaben, z. B. Schulen und Spitäler, als Behörden gelten. Dabei umfasst «Bearbeiten» jeden Umgang mit Personendaten, wie das Beschaffen,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

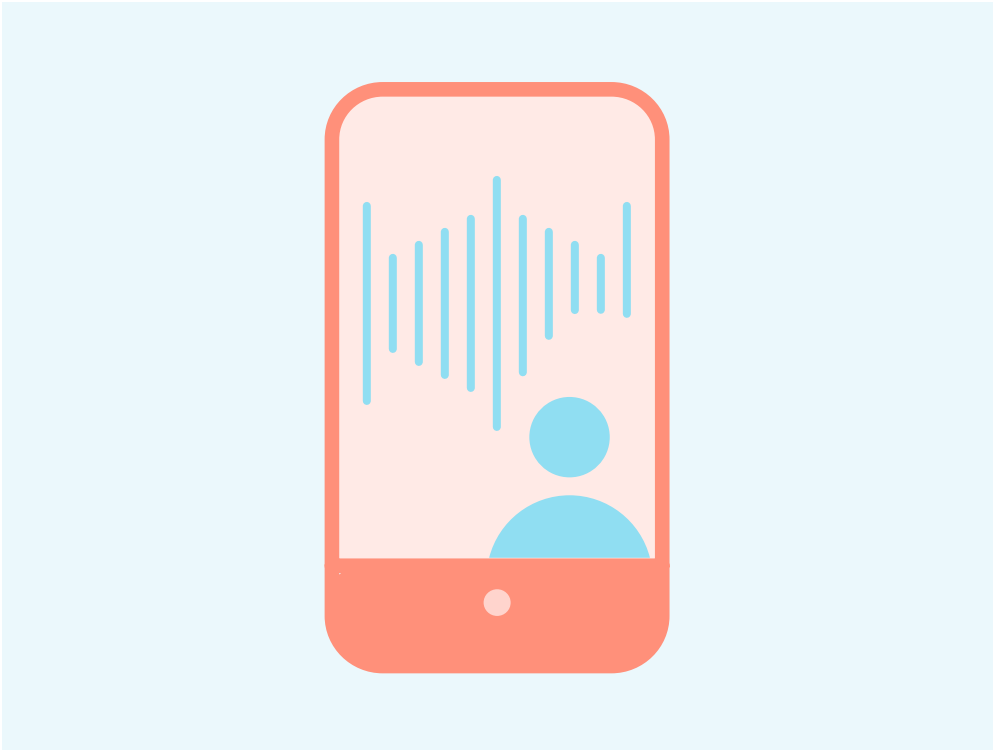
3 Verantwortung und Aufsicht

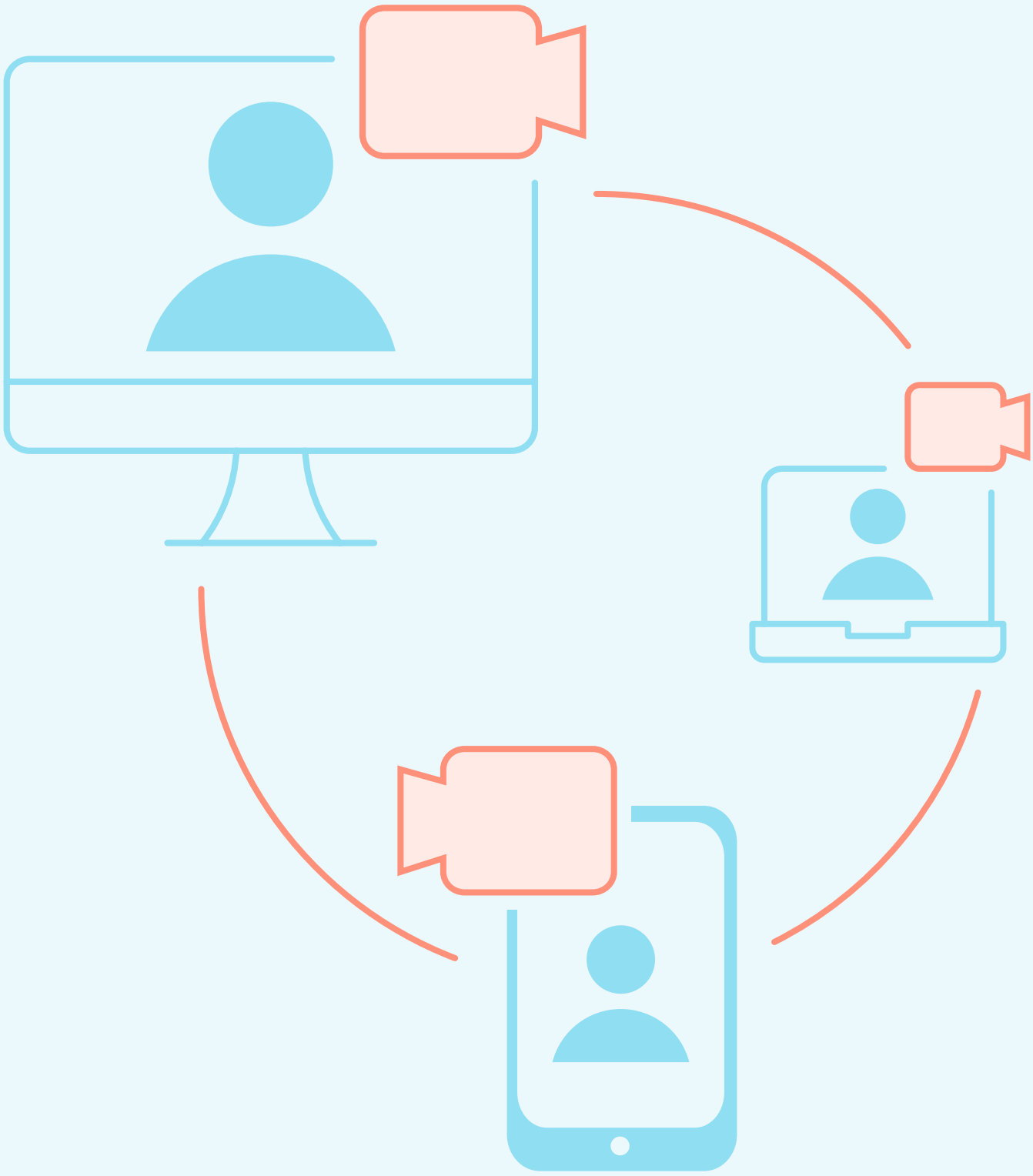
Für den Datenschutz ist jene Behörde verantwortlich, welche die Personendaten zur Erfüllung ihrer gesetzlichen Aufgaben bearbeitet oder von einem Dritten bearbeiten lässt. Sie muss dafür sorgen, dass die Vorschriften über den Datenschutz eingehalten werden und die Datensicherheit gewährleistet ist. Dies 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 2021 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), 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 sämtlichen 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 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.

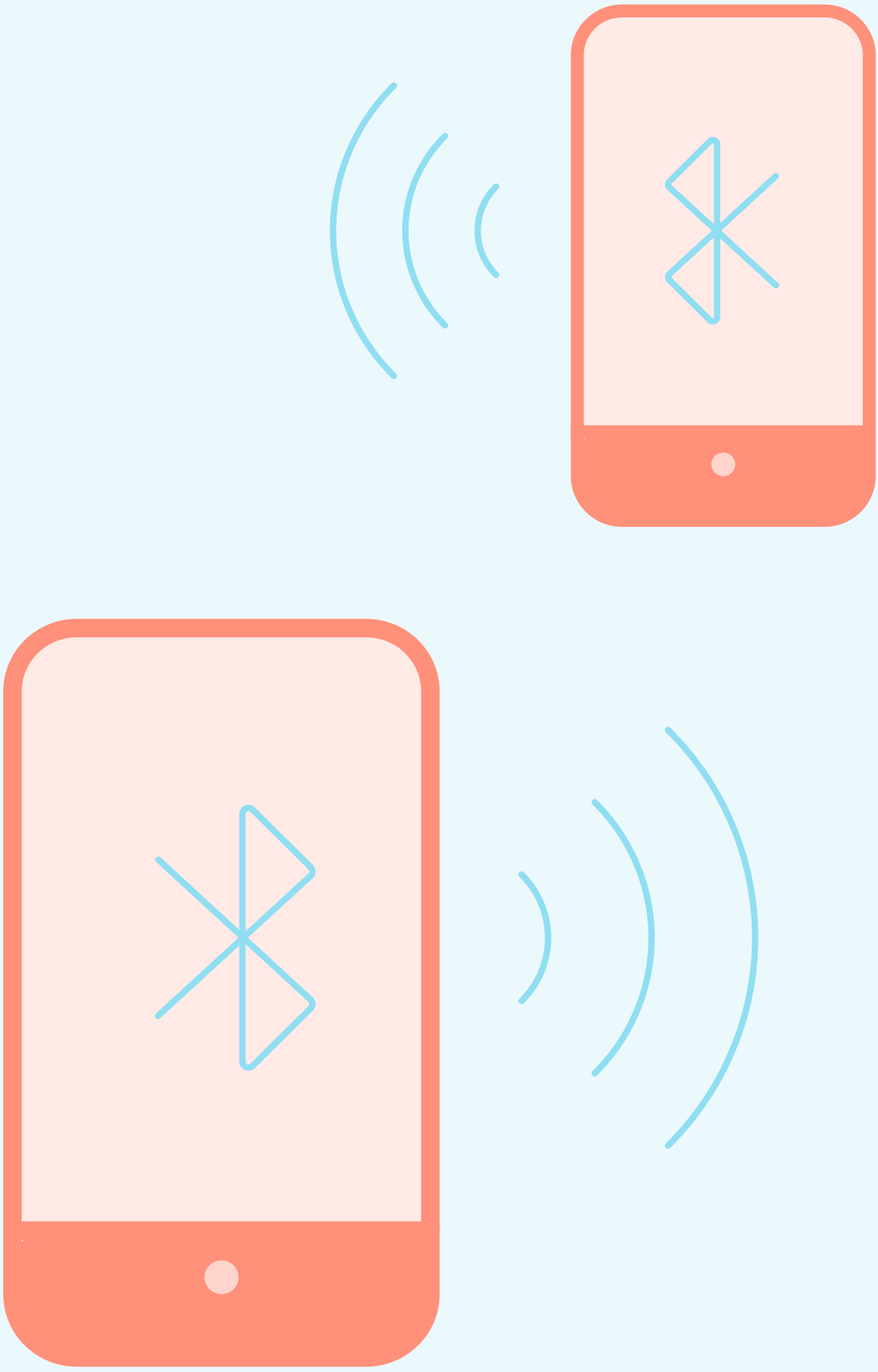
Angesichts der weiterhin stark zunehmenden Arbeitslast insbesondere im Bereich der Vorabkontrollen (siehe dazu Ziff. 6.4.1) prüft die DSA derzeit, ob sie dem Grossen Rat im Rahmen des Voranschlags 2023 den Antrag auf Bewilligung einer zusätzlichen Vollzeitstelle unterbreiten wird.

Im Jahr 2021 betrug der Betriebsaufwand der DSA insgesamt TCHF 243. Davon wurden ca. 88 % (TCHF 215) für externe Dienstleistungen zur Unterstützung von Informatikprüfungen eingesetzt. Aufgrund eines Versehens konnten drei Rechnungen über insgesamt ca. TCHF 70 nicht mehr rechtzeitig verbucht werden; die DSA wird darum in der Staatsrechnung 2021 des Kantons Bern nur einen Betriebsaufwand von TCHF 174 ausweisen und das Budget für das Jahr 2022 im Umfang der nachträglich verbuchten Rechnungen überschreiten.

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 [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, 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 die 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 sowie zur Abfederung derer Auswirkungen auf das gesellschaftliche und wirtschaftliche Leben beschäftigten die DSA auch im Jahr 2021 sehr regelmässig und in unterschiedlichen Tätigkeitsbereichen. Sie bildeten damit ein Schwerpunktthema, zu dem hier vorweg und aufgabenübergreifend berichtet werden soll.

6.1.1 Beratung Behörden

Corona-Testung

Eine Massnahme zur Bekämpfung der Corona-Pandemie ist das Testen von Personen mit und ohne Krankheitssymptomen, um möglichst alle Ansteckungen zu identifizieren. Die DSA unterstützte die GSI und die BKD bereits im Vorfeld zu formellen Vorabkontrollen bei der datenschutzkonformen Einführung der Massentestung an den Schulen und von Betriebszertifikaten an den Hochschulen (siehe zu beidem Ziff. 6.1.4) sowie beim Einsatz des mobilen «Test-Trucks» in den Gemeinden. Dabei formulierte die DSA Empfehlungen an die betroffenen Gemeinden, worauf zu achten ist, wenn Gemeindemitarbeitende im Namen von Personen ohne Internet-Erfahrung die Online-Anmeldung zum Test vornehmen und deren Testergebnisse entgegennehmen.

Zentrale Kontaktdatenbank

Im Hinblick auf die Wiedereröffnung der Innenräume von Restaurants per Ende Mai 2021 gelangte die GSI mit der Anfrage an die DSA, ob und unter welchen Voraussetzungen eine zentrale Datenbank für die Kontaktdaten der Gäste zulässig wäre. Nach Bundesrecht waren die Restaurationsbetreiber/innen verpflichtet, die Daten zu erheben, während 14 Tagen aufzubewahren und auf Verlagen des Kantonsarztamtes unverzüglich an dieses zu übermitteln. Die GSI hatte allerdings die Erfahrung gemacht, dass die Restaurationsbetreiber/innen im Ernstfall oftmals nur schwer erreichbar oder die eingereichten Gästelisten unvollständig waren; deshalb sollten die Daten neu laufend an sie übermittelt werden und bei Bedarf sofort zur Verfügung stehen. Die DSA gelangte zur

Ansicht, dass sich die kantonale Massnahme auf das EpG stützen lasse, sofern mehrere Voraussetzungen erfüllt werden: Die Datenbank muss in der bernischen Covid-19 Verordnung ausdrücklich vorgesehen werden, wo auch die Vorgaben zu formulieren sind, um den Eingriff in die Rechte der betroffenen Personen so gering wie möglich zu halten (Verwendung nur für das Contact-Tracing und nur nach einem konkreten gesundheitsrelevanten Ereignis, Vernichtung nach 14 Tagen, Vorabkontrolle der technischen und organisatorischen Massnahmen zur Sicherstellung dieser Vorgaben durch die DSA [siehe dazu Ziff. 6.1.4]). Zudem kündigte die DSA bereits an, die Datenbank nach der Inbetriebnahme einem Audit zu unterziehen (siehe dazu Ziff. 6.5).

Gegen die vom Regierungsrat gemäss den Vorgaben der DSA verabschiedete Änderung der Covid-19 Verordnung erhob eine private Person Beschwerde beim Bundesgericht. Aus ihrer Sicht durfte der Kanton Bern keine über das Bundesrecht hinausgehende Regelung treffen, sie erachtete die Rechtsgrundlage als ungenügend und die Vorratsdatenspeicherung als unverhältnismässig. Mit Urteil 2C_369/2021 vom 22.09.2021 beurteilte das Bundesgericht die Regelung als rechtmässig und wies die Beschwerde ab.

Die zentrale Kontaktdatenbank führte innerhalb weniger Tage zu mehreren parlamentarischen Interpellationen (093-2021, 097-2021 und 102-2021), welche teils auch die Frage der Datensicherheit adressierten und bei deren Beantwortung die DSA die GSI ebenfalls unterstützte.

Schnittstelle zwischen den Applikationen «SORMAS/TRACY» und «VacMe»

Für das Contact-Tracing verwendet der Kanton Bern die vom Bundesamt für Gesundheit (BAG) empfohlene Applikation SORMAS mit einer kantonseigenen Erweiterung TRACY, die Planung und Dokumentation der Covid-19-Impfungen erfolgt mit der Applikation VacMe. Beide Applikationen beinhalten je eine Personendatensammlung. Seit März 2021 sieht Art. 3a des Covid-19-Gesetzes des Bundes vor, dass durch eine Impfung hinreichend geschützten Personen keine Quarantäne auferlegt wird. Zudem müssen die Kantone Impfdurchbrüche an das BAG melden. Deshalb erkundigte sich die GSI bei der DSA, unter welchen Voraussetzungen Daten über eine Schnittstelle von VacMe an SORMAS/TRACY übermittelt werden dürfen. Die DSA zeigte der GSI allgemein auf, welche datenschutzrechtlichen Vorgaben zu berücksichtigen sind. Die konkrete Umsetzung des Vorhabens prüft die DSA im Rahmen der Vorabkontrolle von SORMAS/TRACY, welche derzeit noch hängig ist (siehe dazu Ziff. 6.1.4).

Zertifikatspflicht für Mitarbeitende von öffentlichen Arbeitgebern

Der DSA wurde die Frage unterbreitet, unter welchen Voraussetzungen für Mitarbeitende der kantonalen Verwaltung, einer Landeskirche, von Einwohner-

oder Kirchgemeinden eine Zertifikatspflicht eingeführt werden dürfte. Nach einem Meinungsaustausch mit dem Personalamt und dem AGR gelangte die DSA zum Schluss, dass auch öffentlich-rechtliche Arbeitgeber gestützt auf die massgebenden bundesrechtlichen Erlasse (Arbeitsgesetzgebung und Covid-19-Verordnung besondere Lage) eine Zertifikatspflicht anordnen dürfen, sofern die dortigen Voraussetzungen erfüllt sind. Das KDSG anerkennt auch für die Bearbeitung von besonders schützenswerten Daten sog. «indirekte» Rechtsgrundlagen, welche eine Aufgabe (wie die Fürsorgepflicht des Arbeitgebers) statuieren, zu deren Erfüllung die Datenbearbeitung zwingend notwendig ist. Die DSA wies jedoch klar darauf hin, dass eine solche Anordnung nur dann zulässig ist, wenn sie auch verhältnismässig ist; dies ist nur dann der Fall, wenn eine Zertifikatspflicht im konkreten Arbeitsumfeld notwendig ist, um angemessene Schutzmassnahmen festzulegen oder ein Testkonzept nach der Covid-Verordnung besondere Lage umzusetzen.

6.1.2 Beratung betroffene Personen

Ermittlung und direkte Ansprache der ungeimpften Personen?

Stellvertretend für die betroffenen Personen erkundigte sich die SRF Tagesschau, ob es – wie an einem «Point-de-Presse» des Bundes als Idee vorgeschlagen – zulässig wäre, dass die Kantone die ungeimpften Personen ermitteln und telefonisch kontaktieren würden. Die Antwort war sehr klar: Solange es der Gesetzgeber nicht erlaubt, wäre bei einer freiwilligen Impfung schon die Ermittlung der Ungeimpften unzulässig. Dafür müssten die Einwohnerregister mit den (im Kanton Bern in VacMe) vorhandenen Impfdaten zusammengeführt und festgestellt werden, wer nicht in beiden Datenbeständen vorkommt. Damit würden die Daten für einen völlig neuen Zweck verwendet, welchem die betroffenen Personen kaum zustimmen würden. Dies gilt auch für deren Telefonnummern, soweit diese den kantonalen Behörden überhaupt bekannt sind.

Anrechnung von Arbeitszeit für die Covid-19-Impfung

Seit Ende März 2021 erlaubt der Kanton Bern seinen Mitarbeitenden die Anrechnung von bis zu einer Stunde Arbeitszeit pro Impfung. Der DSA wurde die Frage unterbreitet, ob es datenschutzrechtlich zulässig sei, im Zeiterfassungssystem einen Vermerk «Corona-Impfung» zu verlangen, was die DSA bejahte: Anders als bei Krankheit oder Unfall besteht bei einer vorsorglichen Impfung kein gesetzlicher Anspruch auf eine Anrechnung von Arbeitszeit, so dass es sich um eine freiwillige Leistung des Arbeitgebers zu einem bestimmten Zweck handelt. Für Mitarbeitende, die – ebenfalls freiwillig – von jenem Angebot Gebrauch machen, ist es zumutbar, dass sie bestätigen, die Stunde zum vorgesehenen Zweck und

nicht beliebig anders eingesetzt zu haben. Der Arbeitgeber bzw. seine Personaladministration darf die Angabe jedoch ebenfalls nur zur Überprüfung der Arbeitszeit und nicht zu anderen Zwecken verwenden und muss sie entsprechend vertraulich behandeln.

6.1.3 Formelle Stellungnahmen

Änderungen der Covid-19 Verordnung des Kantons Bern

Im Jahr 2021 wurde die kantonale Covid-19 Verordnung insgesamt 18 Mal geändert, wobei zahlreiche Änderungen auch den Datenschutz betrafen. Nebst der Schaffung der Rechtsgrundlagen für die zentrale Kontaktdatenbank (siehe dazu Ziff. 6.1.1) wurden die Hochschulen nach der Einführung der Zertifikatspflicht durch den Bundesrat in der kantonalen Verordnung ermächtigt, von überprüften Personen Name, Vorname, Geburtsdatum und Ablaufdatum des Zertifikats zu registrieren, um wiederholte Überprüfungen vermeiden zu können; wichtig war dabei die Vorgabe, dass die Daten nach Ablauf der Gültigkeitsdauer unverzüglich zu löschen sind. Im Dezember führte der Kanton Bern eine Zertifikats- oder regelmässige Testpflicht für die Angestellten von Spitälern, Alters- und Pflegeheimen sowie Spitex-Organisationen ein. Auch vor dem Erlass dieser Regelung trug die DSA im Austausch mit den beteiligten Direktionen dazu bei, einen möglichst einfachen, aber datenschutzkonformen Erlasstext zu erreichen.

Kantonales Gesetz über die Massnahmen im Kulturbereich (Covid-19)

Bei der verwaltungsinternen Vorbereitung eines Gesetzes über die Massnahmen im Kulturbereich im Zusammenhang mit der Covid-19-Epidemie stellte die DSA sicher, dass eine in der bisherigen Einführungsverordnung zur eidgenössischen Covid-19-Gesetzgebung im Kulturbereich enthaltene Vorschrift auch in das neue Gesetz überführt wurde. Die Verordnung und neu das Gesetz erlauben den Austausch aller benötigten Personendaten unter den zuständigen Bundes-, Kantons- und Gemeindebehörden, worüber – dies das Anliegen der DSA – die Gesuchstellenden angemessen zu informieren sind.

Verschiedene Konsultationen zum Bundesrecht

Das EpG verpflichtet den Bundesrat bei einer besonderen Lage zur Anhörung der Kantone, bevor er neue Massnahmen anordnet. Deshalb fanden im Jahr 2021 zahlreiche Konsultationen – teils mit einer Antwortfrist von zwei Arbeitstagen – der Kantone statt, in die der Kanton Bern auch die DSA involvierte, damit sich diese äussern konnte, wenn immer datenschutzrechtliche Fragen betroffen waren.

Beim Konzept «Impf-Offensive» stellte sich der Kanton Bern auf Antrag der DSA klar gegen den Vorschlag einer individuellen Information von ungeimpften Personen, weil hierfür eine genügende Rechtsgrundlage fehlte (siehe dazu Ziff. 6.1.2).

Einer Ergänzung der SwissCovid-App mit einer Funktion zur nachträglichen, anonymen Benachrichtigung der Besucher/innen von Veranstaltungen über eine mögliche Covid-19-Ansteckung an der Veranstaltung konnte die DSA zustimmen, falls – wofür der Bund verantwortlich ist – die technische Umsetzung korrekt erfolgt. Weil die Nutzung der SwissCovid-App auch zu diesem Zweck freiwillig bleibt, kann davon ausgegangen werden, dass die betroffenen Personen den Datenbearbeitungen zustimmen.

Für den internationalen Personenverkehr schlug der Bund vor, dass die Kantone ein System einführen, damit ihnen die Testresultate der eingereisten Personen übermittelt werden können. Dies lehnte der Kanton Bern auch aus Datenschutzgründen ab: Einerseits kennen die Kantone weder die Personalien noch den Impfstatus aller eingereisten Personen. Andererseits würde die Implementierung einer datenschutzkonformen neuen Lösung grosse Aufwände einschliesslich einer Vorabkontrolle durch die DSA erfordern, was die Kantone nicht innert nützlicher Frist zu leisten imstande wären.

6.1.4 Vorabkontrollen

Präventive Massentests an Schulen und Hochschulen

Im Hinblick auf die Durchführung von präventiven Massentests an den Berner Volksschulen und der Sekundarstufe II informierte die GSI die DSA über den geplanten softwaregestützten Prozess im Falle von positiven Pooltests und legte ihr die Fachapplikation PROCESS zur Vorabkontrolle vor. Diese konnte nach Behebung diverser Befunde positiv abgeschlossen werden. Die DSA begleitete die GSI auch nach einem erfolgten Systemwechsel hin zum sog. Ausbruchstesten und wird die neuen Prozesse aus datenschutzrechtlicher Perspektive prüfen, sobald ihr die erforderlichen Unterlagen zur Vorabkontrolle vorgelegt werden.

Im Herbst 2021 führte der Bundesrat die Zertifikatspflicht für den Besuch von Lehrveranstaltungen an Hochschulen ein. In sehr kurzer Zeit errichteten die Hochschulen für ihre Studierenden (und Mitarbeitenden) eigene Testmöglichkeiten. Die Universität Bern stellte der DSA das beabsichtigte Testprozedere – Zugang nur mit Legitimations- bzw. Personalausweis, Probenentnahme vor Ort, Datenerfassung auf einer Plattform und Laborauswertung im Uni-Institut für Infektionskrankheiten – in einer Telefonkonferenz vor und reichte anschliessend die notwendige ISDS-Dokumentation zur Vorabkontrolle ein. Diese konnte mit zwei Befunden mittlerer Wesentlichkeit und einem tief bewerteten Befund positiv abgeschlossen werden.

Zentrale Kontaktdatenbank

Mit der Wiedereröffnung der Innenbereiche von Restaurants per Mai 2021 wurde die Zentrale Restaurant- und Event-Datenbank (ZRDB) zur Identifizierung und Benachrichtigung ansteckungsverdächtiger Personen in Betrieb genommen (siehe zur Frage der Rechtmässigkeit Ziff. 6.1.1). Wer nach dem Bundesrecht zur Erhebung von Kontaktdaten verpflichtet war – nebst den Restaurants waren dies auch Diskotheken und Tanzlokale –, musste die Kontaktdaten täglich elektronisch an die zentrale Datenbank übermitteln. Wie von der kantonalen Covid-19 Verordnung verlangt, unterbreitete die GSI die ISDS-Unterlagen Ende Mai zur Vorabkontrolle durch die DSA.

Da sich die zeitlich verspätete Vorlage der Unterlagen bereits abgezeichnet hatte und die DSA bereit war, einer vorzeitigen Inbetriebnahme zuzustimmen, sofern bestimmte zwingende Anforderungen erfüllt wurden, waren die wichtigsten technischen und organisatorischen Massnahmen bereits vorgängig festgelegt worden: So werden die Daten so verschlüsselt, dass Abfragen nicht nach Personen möglich sind (was die Erstellung eines Profils ermöglichen würde), sondern nur nach Ort und Zeit. Nur dazu berechtigte Mitglieder des Contact-Tracing-Teams können nach Freigabe durch eine epidemiologische Fachperson im Einzelfall Abfragen durchführen und die personenbezogenen Datensätze in der Anwendung TRACY entschlüsseln. Die Aufbewahrung der in der Datenbank gehaltenen Personendaten ist auf 14 Tage beschränkt.

In den nachgereichten ISDS-Unterlagen stellte die DSA mehrere Befunde mit hoher Wesentlichkeit fest, welche primär fehlende bzw. zu wenig detaillierte Beschreibungen zu datenschutzrechtlich relevanten Fragen betrafen. Nach mehreren Verzögerungsanzeigen reichte die GSI Ende Oktober 2021 ihre Stellungnahme ein. Die Prüfung dieser Stellungnahme durch die DSA war per Ende Berichtsjahr noch hängig.

Fachapplikation «SORMAS/TRACY» (Covid-19 Kontaktmanagement)

Für das Covid-19 Kontaktmanagement verwendet die verantwortliche GSI seit dem Herbst 2020 die vom Bund empfohlene und zur Verfügung gestellte Fachapplikation SORMAS. Die GSI ergänzte die Applikation anfangs 2021 mit der vom Kanton Bern selber entwickelten Power-App TRACY. Im Rahmen des Kontaktmanagements bearbeitet die GSI mit den Applikationen SORMAS/TRACY Gesundheitsdaten und damit besonders schützenwerte Personendaten der betroffenen Personen.

Die ersten ISDS-Dokumente zu SORMAS/TRACY reichte die GSI im Frühjahr 2021 bei der DSA zwecks Durchführung einer (nachträglichen) Vorabkontrolle ein. Die DSA meldete der GSI daraufhin dutzende Befunde betreffend ISDS. Aufgrund der unbeständigen Rahmenbedingungen im Kontaktmanagement und

fehlender Angaben konnte die DSA die Vorabkontrolle bislang nicht abschliessen. Der datenschutzkonforme Betrieb der genannten Applikationen ist daher nach wie vor nicht gewährleistet. Gerade mit Blick auf die in SORMAS/TRACY bearbeiteten besonders schützenswerten Personendaten ist dieser Zustand sehr problematisch und weder für die DSA noch für die verantwortliche GSI zufriedenstellend.

Für das Jahr 2022 hat die GSI der DSA Änderungen im Bereich des Kontaktmanagements in Aussicht gestellt; die DSA ist zuversichtlich, zusammen mit der GSI die Vorabkontrolle im Verlauf dieses Jahres zu einem positiven Abschluss führen zu können.

Fachapplikation «VacMe» (Digitale Lösung Covid-19 Impfung)

Für die Planung und Dokumentation der Covid-19 Impfungen im Kanton Bern verwendet die GSI die hierfür eigens für den Kanton Bern entwickelte Applikation VacMe. Wie beim Kontaktmanagement ist auch die Durchführung der Covid-19 Impfung sich kurzfristig ändernden Rahmenbedingungen unterworfen. Dennoch gelang es der DSA mit Unterstützung der VacMe-Projektleitung, die Vorabkontrolle innert Jahresfrist zu einem positiven Abschluss zu bringen. Der datenschutzkonforme Betrieb von VacMe ist, soweit ersichtlich und unter Berücksichtigung der Gesamtumstände, gewährleistet.

Von den von der DSA festgestellten Befunden ist insbesondere die fehlende gesetzliche Grundlage hervorzuheben. Für die im konkreten Fall zur Prüfung vorgelegten Bearbeitungen von (besonders schützenswerten) Personendaten fehlt auf kantonaler wie auch auf Bundesebene eine genügende gesetzliche Grundlage. Der Kanton Bern verlangt zwar für die Impfung eine Einwilligung zur Datenbearbeitung; diese erfolgt grundsätzlich auf freiwilliger Basis (der impfwilligen Bevölkerung) und sie wird für eine hinreichend konkrete und klar umschriebene Personendatenbearbeitung erteilt. Eine fehlende gesetzliche Grundlage vermag jedoch auch eine solche Einwilligung nicht vollständig zu ersetzen. Aus diesem Grund erliess die DSA die Empfehlung, der Kanton Bern solle – jedenfalls im Hinblick auf künftige neue Pandemien, welche mit einem kantonalen Impfprogramm bewältigt werden sollen – die notwendige formellgesetzliche Grundlage erlassen.

Videoüberwachung eines Impfzentrums

Für die Impfzentren im Wankdorf und bei der BernExpo waren nebst der Überwachung durch die Securitas zunächst umfangreiche Videoüberwachungen vorgesehen. Videoüberwachungen zum Schutz von öffentlichen Gebäuden und ihren Benutzer/innen unterliegen im Rahmen des Rückspracheverfahrens nach Polizeigesetz (PolG) einer datenschutzrechtlichen Prüfung (siehe dazu

auch Ziff. 6.4.2). Mit Blick auf die zeitliche Dringlichkeit trug die DSA mit Erklärungen und einem Vorziehen des Geschäfts zur Beschleunigung des Vorabkontrollverfahrens bei. Der Prüfbericht ergab mehrere Befunde, die für einen datenschutzkonformen Betrieb zu verbessern gewesen wären. Daraufhin bewertete der Sonderstab die Sicherheitsrisiken für die Impfzentren neu und gelangte zum Schluss, dass auf die Videoüberwachung verzichtet werden kann, worauf die betreffenden Anlagen zurückgebaut wurden.

6.2 Beratung

6.2.1 Behörden

Audiovisuelle Übertragung von Lehrveranstaltungen der Hochschulen

Die Hochschulen möchten künftig – also auch nach der Pandemie – Lehrveranstaltungen audiovisuell übertragen und gelangten deshalb mit dem Thema an die DSA. Diese prüfte die im Hochschulbereich bestehenden Rechtsgrundlagen und gelangte in ihrer Ersteinschätzung zum Ergebnis, dass eine audiovisuelle Übertragung von Lehrveranstaltungen unter Beachtung der allgemeinen datenschutzrechtlichen Prinzipien, insbesondere der Wahrung der Verhältnismässigkeit, grundsätzlich zulässig ist. Nach Ansicht der DSA lässt sich die verlangte (indirekte) Rechtsgrundlage aus den gesetzlichen Aufgaben der jeweiligen Hochschule ableiten. Die DSA will sich jedoch für eine finale Einschätzung noch mit anderen Datenschutzaufsichtsstellen von Hochschul-Kantonen austauschen.

Digitale Religionslandkarte des Kantons Bern

Der Beauftragte für kirchliche und religiöse Angelegenheiten fragte die DSA an, welche datenschutzrechtlichen Anforderungen beim Aufbau einer digitalen Religionslandkarte zu beachten sind. Bislang gilt das KDSG auch noch für juristische Personen, weshalb die Bearbeitung der (besonders schützenswerten) Daten von Religionsgemeinschaften einer genügenden Rechtsgrundlage bedarf. Die verfassungsmässige Zuständigkeit der Kantone zur Gestaltung des Verhältnisses zwischen dem Staat einerseits und den Kirchen und anderen Religionsgemeinschaften andererseits beinhaltet auch das Weiterentwickeln jenes Verhältnisses. Auf der Grundlage dieser allgemeinen Aufgabennorm beurteilte die DSA eine Bearbeitung von Basisdaten unter der Bedingung als zulässig, dass die einzelnen Religionsgemeinschaften zustimmen und ihre Zustimmung auch jederzeit widerrufen können. Für weitergehende Datenbearbeitungen, z. B. im

Rahmen eines Monitorings, empfahl die DSA, es sei eine ausdrückliche Rechtsgrundlage zu schaffen bzw. dies mindestens zu prüfen.

Forschungsprivileg für private Familienforschung

Eine Privatperson ersuchte für eine Familienbiografie um Einsicht in Gemeinderatsprotokolle, um die damaligen politischen Abläufe zu verstehen und miteinbeziehen zu können. Bis zum Ablauf der gesetzlichen Schutzfrist sind solche Protokolle nicht allgemein zugänglich, das Archivgesetz (ArchG) sieht aber unter Verweis auf das KDSG einen früheren Zugang zu Forschungszwecken zu. Das AGR unterbreitete der DSA die Frage, ob auch private Familienforschung als wissenschaftliche Forschung im Sinne des Gesetzes gilt. In einem ähnlich gelagerten Fall hatte das Verwaltungsgericht auf den Forschungsbegriff des Bundes verwiesen, wonach wissenschaftliche Forschung grundsätzlich auch aus individuellen Interessen erfolgen könne (VGE 100.2010.335). Deshalb erachtete es die DSA als möglich, ein Familienforschungsprojekt mit einer gewissen historisch-gesellschaftlichen Bedeutung als wissenschaftlich anzusehen. Sie wies jedoch auch darauf hin, dass in einer Vereinbarung die nach KDSG für eine Datenbekanntgabe nötigen Datenschutzmassnahmen zu regeln sind.

Änderung des Archivgesetzes

Die DSA wurde vom Staatsarchiv (StAB) eng in die verwaltungsinternen Vorarbeiten zur Revision des ArchG einbezogen. Sie nahm in zwei Arbeitsgruppen Einsitz, welche sich einerseits mit allgemeinen Fragen der Terminologie und Systematik (und dabei insbesondere mit der Koordination zwischen Archiv- und Datenschutzrecht) und andererseits mit der Frage der Archivierung von Psychiatrieakten befassten, und vertiefte Sonderfragen – namentlich zur Schutzfrist von Unterlagen mit besonders schützenswerten Personendaten und zu den Auswirkungen von gesetzlichen Geheimhaltungspflichten – im bilateralen Austausch mit dem StAB. Dies hat sich sehr gelohnt: Alle wesentlichen Datenschutzanliegen konnten bereits informell eingebracht und abgestimmt werden, so dass die DSA im formellen Mitberichtsverfahren nur noch untergeordnete Anträge und Hinweise anzubringen hatte.

Änderung des kantonalen Datenschutzgesetzes

Das KDSG muss an die Vorgaben aus dem europäischen Recht – namentlich einer Änderung der Datenschutzkonvention des Europarats und der auch für die Schweiz verbindlichen Richtlinie (EU) 2016/680 im Bereich des Strafrechts – angepasst werden; dabei soll auch eine Modernisierung im Lichte der technologischen Entwicklung erfolgen. Im Rahmen der verwaltungsinternen Vorbereitung der Vorlage brachte sich die DSA in zwei direktionsübergreifenden

Arbeitsgruppen beratend ein. Neben den materiellen Fragen im Bereich des Datenschutzes ging bzw. geht es auch um politische Fragen (namentlich die Wahl der oder des Datenschutzbeauftragten und die parlamentarische Aufsicht über diese oder diesen) und um die künftige Organisation der Datenschutzaufsicht in den Gemeinden (siehe dazu Ziff. 6.6.2).

Einführung von «Microsoft 365» in der Kantonsverwaltung

Der Einsatz von Cloud-Services ist den Behörden grundsätzlich nicht verwehrt, er bringt aber eine Reihe von besonderen Herausforderungen und Risiken namentlich für die Vertraulichkeit der Daten, welche vorgängig sorgfältig geprüft und durch geeignete Massnahmen auf ein tragbares Mass reduziert werden müssen. Zu diesen Risiken gehören namentlich ein fehlender Gestaltungsspielraum bei weitestgehend standardisierten Verträgen, die Datenbearbeitung in Staaten ohne angemessenen Datenschutz, der Einsatz von ungenügend bekannten Subunternehmen (teils ebenfalls in solchen Staaten), die Bearbeitung von Benutzerdaten für eigene Zwecke des Cloud-Anbieters sowie der mögliche Zugriff von ausländischen Behörden.

Zur Umsetzung der von der DSA verlangten Zwei-Faktoren-Authentifikation, wonach für den Zugang zu besonders schützenswerten Personendaten nebst Benutzername und Passwort ein weiteres Authentisierungsmerkmal erforderlich ist, war ein Produkt von Microsoft evaluiert worden, das auf den Cloud-Services «Azure Active Directory» und «Azure Multi-Factor Authentication» beruht. Im intensiven Austausch innerhalb der Verwaltung und mit Vertretern von Microsoft mussten zahlreiche rechtliche, technische und organisatorische Fragen geklärt werden, um die oben erwähnten Risiken bewerten und mit geeigneten Massnahmen – wie dem Verzicht auf den Einsatz einer Authentifikation mittels SMS oder Sprachnachrichten, welche einen Datentransfer in die USA erfordert hätten – adressieren zu können. Die verbleibenden Restrisiken erschienen auch der DSA als tragbar und wurden durch formellen Beschluss der KAIO-Geschäftsleitung ausdrücklich akzeptiert.

Während es bei der Zwei-Faktoren-Authentifikation zunächst nur um die Benutzerdaten der Kantonsmitarbeitenden ging, betrifft die weitergehende Einführung von Microsoft 365 – d. h. von Diensten zur Kommunikation und Kollaboration sowie von webbasierten Office-Anwendungen – potenziell auch Daten über alle Bürger/innen des Kantons Bern. Darum ist hier eine sehr viel umfassendere Risikoanalyse erforderlich, mit welcher der Regierungsrat das KAIO und die Bedag unter Beizug der DSA beauftragt hat. Der Entscheid über den grundsätzlichen Umfang der Nutzung, die Massnahmen zur Risikominimierung und die getragenen Restrisiken wird ebenfalls der Regierungsrat fällen müssen.

6.2.2. Betroffene Personen

Private Videoüberwachung auf öffentlichem Grund

Eine Person teilte der DSA mit, dass ein privates Unternehmen an einem Hausdach zwei Kameras zur Überwachung des Betriebsgeländes installierte, in deren Fokus jedoch nicht nur der private Grund, sondern auch die öffentliche Strasse lag, und erkundigte sich nach ihren Interventionsmöglichkeiten. Grundsätzlich sind Videoüberwachungen von Privaten nach dem Bundesgesetz über den Datenschutz zu beurteilen und fallen in den Zuständigkeitsbereich des EDÖB. Da hier aber auch die Strasse und damit der öffentliche Boden der Gemeinde betroffen war, konnte die Person an die Gemeindebehörden gelangen, damit diese den Sachverhalt klären und vom Kamerabetreiber verlangen konnte, den Strassenbereich nicht mehr aufzunehmen.

Datenbekanntgabe an das Brustkrebsfrüherkennungsprogramm «donna»

Eine Frau gelangte mit der Frage an die DSA, ob es zulässig war, dass der Kanton Bern ihre Daten an das präventive Mammografie-Screening-Programm «donna» bekanntgab. Laut dem bernischen Gesundheitsgesetz gehört zur öffentlichen Gesundheitspflege auch die Früherkennung von Krankheiten. Auf dieser Grundlage hatte der Kanton Bern zunächst die Krebsliga Bern mit der Durchführung des Programms zur Früherkennung von Brustkrebs beauftragt, später haben die Kantone St. Gallen, Graubünden, Bern und Solothurn das Programm auf die Krebsliga Ostschweiz übertragen. Auf dieser Grundlage darf die Krebsliga auf die Adressen der Frauen ab 50 zugreifen und diese zur Teilnahme einladen. Jede Frau kann jedoch «donna» mitteilen, dass sie nicht mehr angeschrieben werden möchte und allfällige sie betreffende Daten zu löschen sind.

Falschzustellung von Steuerunterlagen

Eine private Person beschwerte sich bei der DSA über eine Falschzustellung von Steuerunterlagen. Die DSA unterstützte die Person bei deren Schritten zur Klärung und stellte bei den Steuerbehörden Rückfragen zum Vorfall. Es stellte sich heraus, dass eine Post-Retoure bei der Steuerverwaltung zu einer Adressänderung geführt hatte, ohne dass die Adresse von der Steuerbehörde oder der Gemeinde verifiziert worden war. In der Folge gingen mehrere Steuersendungen an falsche Personen. Nach den Interventionen des Anzeigers und der DSA korrigierten die Gemeinde den Adresseintrag und die Steuerverwaltung den Prozess beim Umgang mit Adressänderungen.

Auskunft und Einsicht in eigene Daten bei der Staatsanwaltschaft

Gestützt auf das KDSG erhält jede Person auf Verlangen schriftlich Auskunft über die Daten, die eine Behörde über sie bearbeitet; ebenfalls auf Verlangen erhält sie Einsicht in jene Daten, wenn nicht besondere Umstände vorliegen. Die Staatsanwaltschaft war bereit, einer Person vor Ort Einsicht in die sie betreffenden Akten zu gewähren; eine schriftliche Auskunft wurde ihr dagegen mit der Begründung verweigert, dass die weitergehende Einsicht auch den Anspruch auf Auskunft erfülle. Nach einem kurzen Austausch mit der Staatsanwaltschaft informierte die DSA die Person, dass sie von der Staatsanwaltschaft eine formelle Verfügung zum Antrag auf schriftliche Auskunft verlangen und diese bei der Generalstaatsanwaltschaft anfechten könne. In konkreten Angelegenheiten einzelner Personen kann die DSA zwar die Betroffenen über ihre Rechte beraten und zwischen ihnen und den Behörden vermitteln, sie hat aber kein Weisungsrecht gegenüber den Behörden und vertritt die Personen auch nicht in einem anwaltschaftlichen Sinne.

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 – 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. Zusätzlich zu einem im Vorjahr neu eingeführten Kurs für Mitarbeitende von Kirchgemeindesekretariaten fand im Berichtsjahr auch 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 Auftragsdatenbearbeitung durch Cloud-Anbieter (10. IT-Beschaffungskonferenz der Universität Bern, Workplace Conference 2021 der Schweizerischen Informatikkonferenz [SIK], Schulthess Forum Datenschutz in Städten und Gemeinden 2021), über den Datenschutz im Schulwesen (14. Schweizerischer Datenschutz-

tag der Universität Fribourg) und über Datenschutzfragen während der Pandemie (gemeinsamer Anlass der Swiss DPO Association und der Swiss Healthcare Privacy Professionals).

Zudem präsentierte ein Vertreter der DSA an einem Weiterbildungsanlass der Regierungsstatthalterämter die Grundlagen des Datenschutzes und zeigte die Erfahrungen der DSA mit den Gemeinden und ihren kommunalen Datenschutzaufsichtsstellen auf.

6.3 Formelle Stellungnahmen

Änderung der Volksschulverordnung: Talentkarte

Mit einer Änderung der Volksschulverordnung wurde im musischen Bereich eine Talentkarte für hochbegabte Schüler/innen eingeführt, welche von einer Fachkommission ausgestellt wird und die Eignung der Hochbegabten für den Besuch eines spezifisch-strukturierten Förderprogramms oder Ausbildungsgangs in qualifizierter Form bestätigt. Die DSA wünschte bereits in der Verordnung Anhaltspunkte dafür, welche Personendaten auf der Talentkarte enthalten sein werden. Weil dies im Zeitpunkt der Änderung noch nicht feststand, wird die zuständige BKD die DSA erneut konsultieren, sobald der Entwurf für die Talentkarte erarbeitet wurde, damit die datenschutzrechtlichen Anliegen berücksichtigt werden.

Neues Finanzhaushaltsgesetz

Der im November 2021 vom Regierungsrat an den Grossen Rate verabschiedete Entwurf für ein neues Finanzhaushaltsgesetz enthält detaillierte Bestimmungen zu den Datenbearbeitungen im Finanzinformationssystem und – via indirekte Änderung des Personalgesetzes – im Personalinformationssystem des Kantons Bern. In enger Zusammenarbeit mit der DSA wurden für beide Gesetze die vom KDSG verlangten klaren Rechtsgrundlagen auch für die Bearbeitung von besonders schützenswerten Daten und den Abruf solcher Daten aus zentralen Personendatensammlungen nach dem Personendatensammlungsgesetz (PDSG) geschaffen.

Berechtigungsregeln für zentrale Personendatensammlungen

Zusammen mit dem PDSG traten per 1. März 2021 auch neue Verordnungen über die Gemeinderegisterplattform (GERES V) und über die Zentrale Personenverwaltung in Kraft. Beide Verordnungen sehen vor, dass die Direktionen, die STA und die Justiz innerhalb eines Jahres neue Berechtigungsregeln für ihre Zugriffe

auf die beiden Datensammlungen regeln und der DSA vorgängig zur Stellungnahme unterbreiten müssen. Alle Zugriffe müssen sich auf eine genügende Rechtsgrundlage stützen und zur Erfüllung der gesetzlichen Aufgaben erforderlich sein, was in für die DSA nachvollziehbarer Weise zu begründen ist. Im Berichtsjahr nahm die DSA zu den Berechtigungsregeln der FIN, der DIJ und der GSI je formell Stellung; die STA erlässt keine Berechtigungsregeln, weil sie künftig ohne jene Zugriffe auskommt.

Nebst den kantonalen Behörden beriet die DSA auch Einwohner- und Kirchgemeinden sowie deren Aufsichtsstellen bei der Erstellung bzw. Prüfung von kommunalen Berechtigungsregeln, welche allerdings nur insoweit erforderlich sind, als die benötigten Zugriffe über jene hinausgehen, welche die GERES V im Anhang bereits für alle Gemeinden statuiert.

Änderung der Arbeitsmarktverordnung: Videoaufzeichnungen

Die Arbeitsmarktverordnung enthält neu eine detaillierte Regelung zur Video- und Audioaufzeichnung von Kundengesprächen zum Zweck der Qualitätssicherung und der Weiterbildung von Mitarbeitenden. Eine Aufzeichnung darf nur mit der schriftlichen Einwilligung aller Beteiligten erfolgen, die jederzeit ohne Begründung widerrufen werden kann. Aufzeichnungen dürfen längstens während sechs Monaten aufbewahrt werden und sind auf Verlangen der aufgezeichneten Personen sofort zu vernichten. Die DSA wurde bei der Redaktion der neuen Regelung eng miteinbezogen und hatte daher im formellen Mitberichtsverfahren nur noch einen Hinweis zum Vortrag anzubringen.

Änderung des Informationsgesetzes

Nachdem die DSA bei der verwaltungsinternen Vorbereitung ihre Anliegen – namentlich zur inhaltlichen Abstimmung zwischen dem Informationsgesetz und dem KDSG – vollumfänglich einbringen konnte, konnte sie dem Entwurf im ersten Mitberichtsverfahren und in der Vernehmlassung vollumfänglich zustimmen. Erst im zweiten Mitberichtsverfahren musste sie sich noch einmal gegen eine Änderung zur Wehr setzen, welche die STA auf Antrag einer anderen Direktion angebracht hatte: In Abstimmung mit der DSA enthält der neue Entwurf die Ermächtigung, Informationen von allgemeinem Interesse im Internet bekanntzugeben, auch wenn sie Personendaten enthalten; besteht das öffentliche Interesse an den publizierten Personendaten nicht mehr, sind diese zu entfernen. Weil sich diese Anforderung zwingend aus dem Verfassungsrecht (Verhältnismässigkeitsprinzip) ergibt, genügte der DSA ein blosser Verweis auf das Datenschutzrecht nicht. Dafür bestätigte sie, dass sich die Löschungsverpflichtung nur auf eigene Publikationen der Behörden erstreckte und nicht auf das gesamte Internet, wo die Übernahme von publizierten Inhalten durch Dritte nicht verhindert werden kann.

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 138 Vorabkontrollen und Vorprüfungen (Vorjahr: 123) zu Informatikprojekten bearbeitet und dabei 77 (58) bzw. 55.8 % (47.2) 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.

Kantonales Krebsregister Bern Solothurn (KRBESO)

Seit dem 1. Januar 2020 gilt das neue Krebsregistrierungsgesetz (KRG) des Bundes. Dieses bildet die gesetzliche Grundlage für die flächendeckende, vollzählige und vollständige Datenerfassung von Tumorerkrankungen, Krebsvorstufen und gewissen gutartigen Tumoren. Jeder Kanton ist verantwortlich für die Führung eines kantonalen Krebsregisters im Sinne des KRG. Die Führung der Krebsregister der Kantone Bern und Solothurn (KRBESO) ist dem Institut für Pathologie der Universität Bern übertragen worden. Das KRBESO verwendet für seine Aufgabe neu die vom Bund gratis zur Verfügung gestellte Registrierungssoftware (RSW). Diese löste die bis anhin verwendete Vorgängersoftware NICERStat ab. Das KRBESO ist derzeit das einzige Krebsregister, welches bereits produktiv mit der nationalen RSW arbeitet. Andere Krebsregister nahmen Anpassungen an der Software NICERStat vor, um den Voraussetzungen des KRG zu genügen.

Der Wechsel zur nationalen RSW machte eine Vorabkontrolle erforderlich. Die DSA prüfte die ISDS-Unterlagen des KRBESO und vom Bund und stand hierfür mit der Koordinatorin des KRBESO und mit Vertretern der Abteilung Digitale Transformation des BAG in Kontakt. Aufgrund der starken pandemiebedingten

Auslastung des BAG kam es zu erheblichen Verzögerungen bei erforderlichen Anpassungen von ISDS-Dokumenten des Bundes. Weil die Vorabkontrolle der DSA auch für alle weiteren Kantone interessant war, die später zur nationalen RSW wechseln wollen, intervenierte privatim (siehe dazu Ziff. 6.7) beim BAG und bat um eine zeitnahe Bearbeitung der Fragen, welche das KRSBESO der DSA beantworten musste. Im Dezember 2021 konnte die DSA das Vorabkontrollverfahren schliesslich mit einem positiven Bericht abschliessen.

Videokonferenztools

Beschleunigt durch die Bedürfnisse aufgrund der Heimarbeit während der Pandemie – aber nicht auf diese beschränkt – wurden der DSA gleich mehrere verschiedene Videokonferenztools zur Vorabkontrolle unterbreitet. So führte das KAIO als Ergänzung zu den bestehenden Kommunikationskanälen die Anwendung «Zoom» ein, nachdem der Anbieter zugestimmt hatte, dass der mit der Stiftung SWITCH für den Hochschulbereich abgeschlossene Rahmenvertrag auch für andere öffentliche Organe zur Anwendung gelangte. Für eine datenschutzkonforme Nutzung der Software waren verschiedene Massnahmen zu treffen: So verlangte die DSA, dass die End-zu-End-Verschlüsselung des Datenverkehrs, die zwar gewisse Funktionen einschränkt, aber dafür sicherstellt, dass der Anbieter keinen Zugriff auf die Inhalte hat, als Standard und nicht nur als Option konfiguriert wird. Weil die Benutzerkonten in den USA verwaltet werden, welche nicht als Staat mit einem angemessenen Datenschutzniveau gelten, musste die Kontoeröffnung zudem freiwillig sein, wobei die Benutzer vorgängig klar über den Datentransfer und das Risiko ausländischer Behördenzugriffe informiert werden mussten.

Auch bei der Anwendung «MyJustice» des Amtes für Justizvollzug (AJV), welche vom Programm HIS (Harmonisierung der Informatik in der Strafjustiz) des Bundes und der Kantone evaluiert und empfohlen worden war, verlangte die DSA gewisse Massnahmen, etwa den Ausschluss des Einsatzes für den Bereich der Telemedizin, wo besondere gesetzliche Geheimhaltungspflichten gelten. Im Rahmen der Umstellung der BKD auf den Kantonalen Arbeitsplatz benötigte die BKD die «Microsoft Teams Desktop App», um im bisherigen Umfang die IT-Services von EDUBERN für Schulen der Sekundarstufe II und der Volksschule nutzen zu können. Die Services waren von der DSA im Jahr 2018 auditiert und auf der Grundlage des damaligen Wissensstands als datenschutzkonform beurteilt worden. Nach dem Urteil «Schrems II» des Europäischen Gerichtshofes von 2020, wonach Datenexporte in die USA weitgehend unzulässig sind, und einer vertieften Prüfung des Vertragswerks mit Microsoft war jene Beurteilung in Frage gestellt. Gleichwohl tolerierte die DSA primär aus Gründen des Vertrauensschutzes den Einsatz der Anwendung bis zur ordentlichen Einführung von Microsoft 365 in der Kantonsverwaltung (siehe dazu Ziff. 6.2.1).

Leistungsbewirtschaftung bei Kindern mit besonderem Förder- und Schutzbedarf

Im Hinblick auf das Inkrafttreten des neuen Gesetzes über die Leistungen für Kinder mit besonderem Förder- und Schutzbedarf per Anfang 2022 benötigte das Kantonale Jugendamt ein neues System für die Abwicklung der Bestellungen und der Vorfinanzierung der Leistungen von einer Vielzahl von Leistungserbringern. Das System besteht aus mehreren Komponenten: einem auf dem Portal BE-Login basierenden externen Zugang für Besteller und Leistungserbringer, einer Prozessplattform als Datendrehscheibe sowie einer Geschäftsverwaltungssoftware für die Ablage und Aufbewahrung der einzelnen Geschäfte. Angesichts besonders schützenswerter Angaben zu Kindern war namentlich zu prüfen, mit welchen Massnahmen gewährleistet wird, dass die Daten nicht für Unbefugte zugänglich sind und nach Ablauf der Aufbewahrungsdauer sicher gelöscht werden, soweit keine Archivierung erfolgt.

Nachdem die gleiche Prozessplattform schon von einer zweiten Direktion eingesetzt wurde, regte die DSA beim KAIO und bei der Bedag an, für den Service eine generische ISDS-Dokumentation zu erstellen und der DSA zur Vorabkontrolle zu unterbreiten, auf welche sich dann andere Direktionen und Ämter abstützen können.

Fachapplikation «InfoSearch» der Kantonspolizei

Das PolG und die Strafprozessordnung erlauben unter restriktiven Voraussetzungen eine verdeckte Ermittlung oder Fahndung vor bzw. nach Ausführung eines Verbrechens oder Vergehens. Verdeckte Ermittler/innen, denen die Wahrung der Anonymität zugesichert worden ist, haben Anspruch darauf, dass ihre wahre Identität gegenüber unbefugten Dritten – einschliesslich nicht berechtigten Polizeiangehörigen – geheim gehalten wird und auch nicht in die Verfahrensakten aufgenommen wird. In der Fachapplikation InfoSearch wird die Zusammenarbeit mit in diesem Sinne vertraulichen «Quellen» verwaltet und zusammen mit den verdeckt erhobenen Informationen dokumentiert. Angesichts der sehr hohen Vertraulichkeit der Daten gelangte die DSA bei ihrer ersten Prüfung der ISDS-Unterlagen zu mehreren wesentlichen Feststellungen namentlich zur Datenverschlüsselung, zur Wahrung der Vertraulichkeit gegenüber externen Leistungserbringern und zur sicheren Löschung von nicht mehr benötigten Daten und Backups. Alle Befunde wurden von der KAPO akzeptiert und durch zusätzliche Massnahmen oder Beschreibungen erledigt.

Chatbots

Gleich zwei Ämter reichten ISDS-Unterlagen für die Einführung eines Chatbot ein, welcher Anfragen der Benutzenden mittels erkannter Begriffe automatisch

beantworten soll: Ein Chatbot des Amtes für Sozialversicherungen (ASV) soll hilfesuchenden Bürger/innen grundlegende Fragen zum Anspruch auf Prämienverbilligung bei der Krankenkasse beantworten. Und ein SupportBot des KAIO soll den Mitarbeitenden der Kantonsverwaltung erste Antworten auf ihre Anliegen liefern oder sie zu den betreffenden Informationsseiten lenken. Beiden Fällen war gemeinsam, dass die Bots nicht zur Bearbeitung von Personendaten bestimmt sind, es jedoch nicht mit technischen Mitteln verhindert werden kann, dass die Benutzenden trotzdem Personendaten in das Freitextfeld eingeben. Es musste deshalb sichergestellt werden, dass die Bürger/innen bzw. Kantonsmitarbeitenden vor der Nutzung des Bots unübersehbar und klar verständlich darauf hingewiesen werden, dass sie keine Angaben (wie Namen, Mailadressen, AHV-Nummern und dergl.) eintragen dürfen, welche sie selbst oder andere Personen bestimmbar machen. Im Falle des ASV konnte damit auf eine formelle Vorabkontrolle verzichtet werden, weil sich der Anbieter und seine Server in der Schweiz befinden und die vom Kanton Bern verlangten ISDS-Bedingungen vertraglich vereinbart waren. Das KAIO, das auf Services von internationalen Dienstleistungen zurückgriff, musste in einer formellen Vorabkontrolle darlegen, welche weiteren Massnahmen ergriffen wurden, um die Risiken bei einer nicht bestimmungsgemässen Nutzung des SupportBot zu minimieren.

6.4.2. Videoüberwachungen

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

Amt für Bevölkerungsdienste

Die DSA prüfte erstmals die Videoüberwachung des Amtes für Bevölkerungsdienste (ABEV). Das ABEV ist zuständig für die Aufenthaltsregelung ausländischer Personen, die Gewährung der Nothilfe an abgewiesene Asylsuchende und den Vollzug von Wegweisungen. Mit einer kombinierten Echtzeitüberwachung mit Aufzeichnung werden aus Sicherheitsgründen jene Bereiche überwacht, zu denen Kundinnen und Kunden Zutritt haben. Die Prüfung führte zu mehreren datenschutzrechtlichen Verbesserung. So werden die Besprechungszimmer zwar

grundsätzlich zum Schutz der Mitarbeitenden und der Kundschaft überwacht, die Mitarbeitende können die Aufnahme jedoch unterbrechen lassen, wenn sie diese nicht für nötig halten. Eine neue Weisung erläutert ISDS-Aspekte für die Mitarbeitenden und stellt sicher, dass mit den Kameras keine Mitarbeiterüberwachung erfolgt.

Inselspital

Im Inselspital wurde in mehreren Gebäuden und im Parkhaus der Einsatz neuer Kameras geprüft, welche die bereits bestehende Überwachung ergänzten. Sie sollten entweder zum Schutz der öffentlichen Sicherheit als kombinierte Echtzeitüberwachung mit Aufzeichnung betrieben werden oder zur Gewährleistung der Gesundheit der Patientinnen und Patienten im Rahmen der Aufgabenerfüllung des Spitals eine Echtzeitüberwachung erlauben. Weil bereits der Umstand, dass eine Person als Patientin oder Patient ein Spital besucht, eine Angabe über die Gesundheit der Person darstellt, sind Bilder mit Patient/innen besonders schützenswerte Daten und unterstehen dem Berufsgeheimnis der Gesundheitsfachpersonen. Daraus ergeben sich regelmässig hohe Anforderungen an die Datensicherheit, auf welche die DSA die Verantwortlichen hinweist.

Mobile Videosysteme der Kantonspolizei

Im August 2021 startete die KAPO einen Pilotversuch mit am Körper getragenen Beweissicherungskameras (sog. «Bodycams»). Im Vorjahr hatte die DSA die Frage der gesetzlichen Grundlagen geprüft und sich anlässlich eines Berichts des Regierungsrates dazu geäussert (vgl. dazu Ziff. 6.3 des Jahresberichts 2020). Im Berichtsjahr unterbreitete die KAPO der DSA die ISDS-Unterlagen zum Einsatz von mobilen Videosystemen und dabei auch der Beweissicherungskameras zur Prüfung. Die vorhandenen Rechtsgrundlagen erlauben einen Einsatz dieser Kameras nur dann, wenn ernsthafte Anzeichen bestehen, dass ein Verbrechen oder Vergehen unmittelbar vor der Ausführung steht oder begangen wurde. Deshalb dürfen die Kameras im Einsatz nicht permanent laufen, sondern müssen von den Polizeibeamt/innen im Einzelfall eingeschaltet werden. Entsprechend prüfte die DSA nicht nur die technischen und organisatorischen Massnahmen zum sicheren Umgang mit den Aufzeichnungen, sondern auch die Unterlagen zur Schulung der betreffenden Polizeibeamt/innen.

6.5 Audits

Im Rahmen seines gesetzlichen Auftrags, die Anwendung der Vorschriften über den Datenschutz und die Datensicherheit zu überwachen, führte die DSA im Berichtsjahr insgesamt acht eigene ISDS-Audits durch. Ein weiterer Audit (Fachapplikation GINA-Web) erfolgte in Zusammenarbeit mit der FK. Diese Zusammenarbeit soll im Jahr 2022 weitergeführt und ausgebaut werden.

Zu abgeschlossenen Audits aus den Jahren 2016–2020 begleitete die DSA kontinuierlich die Umsetzung von Verbesserungsmassnahmen. Diese aktive Begleitung stellt eine wirksame und zielführende Standardaufgabe der DSA dar. Diese musste wiederholt feststellen, dass ISDS-Aufgaben eine hohe Aufmerksamkeit von den verantwortlichen Stellen benötigen. Diese Aufmerksamkeit konnte die DSA nicht immer im gewünschten Masse feststellen. Teilweise besteht ein sichtbarer Aufgabenrückstau, teils aufgrund des sonstigen herausfordernden Tagesgeschäfts und teils wegen der ausserordentlichen Rahmenbedingungen aufgrund der behördlichen Massnahmen zur Eindämmung der Pandemie. Eine verzögerte Umsetzung von ISDS-Verbesserungsmassnahmen erhöht grundsätzlich das Risiko, dass auf die sich rasch ändernde Bedrohungslage durch Cyberkriminalität nicht zeitnah und angemessen reagiert werden kann. Die DSA erwartet daher, dass die verantwortlichen Stellen auch das erhöhte Cyberrisiko bei der Priorisierung ihrer Aufgaben berücksichtigen, zumal sowohl Qualität als auch Quantität von kriminellen Cyberaktivitäten im Berichtsjahr weiter zugenommen haben. Die ISDS-Verantwortung tragen dabei ausnahmslos die Stellen, welche Personendaten bearbeiten.

«BE-Net / IPv6»

BE-Net fasst netzwerktechnische Dienstleistungen zusammen, welche das KAIO der kantonalen Verwaltung und weiteren Kunden zur Verfügung stellt. Dazu gehören ein Weitverkehrsnetz (Wide Area Network, WAN), die kabelgebundenen lokalen Netzwerke an den Standorten (Local Area Networks, LAN) und die drahtlosen lokalen Netzwerke an den Standorten (Wireless Local Area Networks, WLAN). Das BE-Net steht an 288 Standorten zur Verfügung, wird neben der Kantonsverwaltung von 48 Schulen und 215 Gemeinden eingesetzt und erreicht circa 37 500 Nutzer/innen. Der BE-Net Betrieb ist an einen externen Dienstleister ausgelagert. Die aktuell für die Datenübertragung zwischen Computersystemen verwendete Netzwerktechnologie Internet Protokoll Version 4 (IPv4) soll mittelfristig durch den Nachfolger Internet Protokoll Version 6 (IPv6) abgelöst werden. Die schrittweise Einführung von IPv6 ist mit erhöhten ISDS-Risiken verbunden.

Der durchgeführte Audit umfasste primär die Beurteilung der Netzwerk- und Sicherheits-Architektur für WAN, LAN, IPv6, Dual-Stack und Tunneling sowie den Strategien und Methoden der IPv6-Netzwerksicherheit und des Datenschutzes. Es erfolgte zudem eine Beurteilung hinsichtlich Netzwerkrobustheit bzw.

Resilienz. Zusätzlich wurde ein technischer Netzwerk-Penetrationstest (Schwachstellenprüfung) durchgeführt.

Das Gesamtergebnis des Audits wies keine erhöhten ISDS-Risiken aus. Dennoch wurden einige Befunde mit mittlerem und tiefem Risiko festgestellt, welche Verbesserungsmassnahmen erfordern. Der Netzwerk-Penetrationstest zeigte auf, dass einige technische Schwachstellen bestehen und diese ausgenutzt werden können. Auch wesentliche Betriebsprozesse müssen verbessert werden. Weiter fehlen nachvollziehbare regelmässige Schwachstellentests. Der durchgeführte Audit erfolgte in einem professionellen und konstruktiven Umfeld.

«BE-Voice» / Telefonie

Das KAIO stellt mit BE-Voice im Rahmen von technischen Dienstleistungen eine einheitliche und standardisierte Telefonie- und Kommunikationsplattform für die Kantonsverwaltung zur Verfügung. BE-Voice beinhaltet das Software-Produkt Skype-for-Business. Die Anzahl der Nutzer/innen liegt bei circa 10 000. Dazu bestehen noch circa 500 physische Telefone (Voice-over-IP-Technologie). Für die Verwaltung und Steuerung der Anrufe auf die Hauptnummern der Ämter und für Service-Nummern sowie Hotlines wird die Fachanwendung Competella eingesetzt. Es bestehen circa 4500 Competella-Nutzer/innen. Der technische Betrieb ist vollständig an externe Dienstleister ausgelagert.

Das Ziel des durchgeführten Audits umfasste die Beurteilung der Sicherheit des Telefonie-Services. Dabei standen die Netzwerk- und Infrastruktur-Architektur für BE-Voice und der Fachanwendung Competella im Zentrum der Prüfungshandlungen. Auch die Einhaltung von Vorgaben und die wirksame Umsetzung von sicheren Konfigurationen wurden beurteilt. Weiter wurden wesentliche Betriebsprozesse sowie die vertraglichen Vereinbarungen geprüft. Ein technischer Penetrationstest (Schwachstellenprüfung) auf selektive, besonders relevante technische BE-Voice Komponenten bzw. Bereiche wurde ebenfalls durchgeführt.

Im Rahmen des Audits wurden in den Prüfbereichen ISDS-Konzept, Konfiguration, Härtung und Sicherheit des Telefonie-Netzwerks sowie Betrieb und Betriebsprozesse als auch bei den Leistungsverträgen Befunde mit einem mittleren ISDS-Risiko festgestellt. Der Penetrationstest zeigte keine kritischen Schwachstellen auf. Das Gesamtergebnis kann als gut bewertet werden. Der BE-Voice Audit konnte in einem professionellen Umfeld durchgeführt werden.

E-Mail Service

Der KAIO zur Verfügung gestellte E-Mail-Service für die Kantonsverwaltung stellt eine einheitliche und standardisierte E-Mail-Dienstleistung dar. Der E-Mail-Service umfasst dabei alle notwendigen technischen Komponenten für die Verwaltung

und Bearbeitung, d.h. Versand und Empfang von E-Mails auf der Basis des Produkts Microsoft Exchange. Eine Secure-Mail-Lösung, welche die sichere End-to-End Verschlüsselung von E-Mails ermöglicht, wird ebenfalls zur Verfügung gestellt. Die technische Umsetzung und der Betrieb der gesamten E-Mail-Lösung erfolgen extern.

Bei diesem Audit stand die nachweisbare Erfüllung der technischen und organisatorischen ISDS-Anforderungen durch die verantwortlichen Leistungserbringer im Fokus. Zusätzlich sollte ein technischer Penetrationstest vorhandene Schwachstellen aufzeigen.

Bei den Prüfungshandlungen wurden in den Prüfbereichen ISDS-Konzept, Infrastrukturarchitektur, Zugriffsmanagement, Schnittstellen und Leistungsverträge sowie beim dedizierten Penetrationstest Befunde mit einem mittleren ISDS-Risiko festgestellt. Der Penetrationstest zeigte auf, dass teilweise Versionen von Verschlüsselungs-Algorithmen verwendet wurden, bei denen Schwachstellen bekannt sind. Auch konnte eine Netzwerkschwachstelle erkannt werden, welche indirekt ein Risiko für den E-Mail-Service darstellt. Der Audit konnte in einem professionellen und freundlichen Umfeld durchgeführt werden.

Service Desk

Der Service Desk (SDK) des KAIO ist für die Mitarbeitenden der kantonalen Verwaltung die erste Anlaufstelle (BE-Support Service) bei Fragen und Störungen im Zusammenhang mit der Informatik und Telekommunikation. Der SDK ist dabei primär für die Behebung von Störungen zuständig. Der SDK führt weitergehende Abklärungen durch oder leitet Störungsmeldungen und Anfragen bei Bedarf an eine zuständige Stelle zur Bearbeitung weiter. Die Anfragen und Störungsmeldungen werden dabei in einem Ticket-System erfasst und bearbeitet. Der SDK verfügt über verschiedene technische Hilfsmittel (Support-Tools) und eine Infrastruktur für die Bearbeitung, Analyse und Behebung von Störungen.

Das Ziel des durchgeführten ISDS-Audits umfasste die Beurteilung der Erfüllung von ISDS-Anforderungen des kantonalen BE-Support Services mit den verwendeten Support-Tools sowie der eingesetzten technischen Infrastruktur.

Das Ergebnis des Audits zeigt auf, dass im Zusammenhang mit der (ISDS-) Schulung der SDK-Mitarbeitenden noch Verbesserungen notwendig sind. Auch wurde festgehalten, dass die ISDS-Vorgaben für den SDK nicht vollständig und verbindlich vorlagen. Die Umsetzung und Kontrolle von SDK ISDS-Vorgaben konnte ebenfalls nicht vollständig nachvollziehbar aufgezeigt werden. Weiter bestehen erhöhte ISDS-Risiken bei der eingesetzten Infrastruktur sowie bei den verwendeten Support-Tools. Das KAIO wird die Verbesserungsmassnahmen zeitnah angehen. Der Audit konnte in einer freundlichen und offenen Atmosphäre durchgeführt werden.

«GINA-Web»

Bei GINA-Web handelt es sich um eine modulare Fachanwendung, welche auf einer sog. Workflow-Engine und Internet-Technologie basiert. Der zentrale Benutzerkreis der Fachanwendung GINA-Web sind die Fachpersonen des AJV, welche mit der Fachanwendung ihre Kern- und Supportprozesse für den Vollzug der Strafen und Massnahmen der eingewiesenen Personen abwickeln. Zusätzlich zum AJV gehören zum Nutzerkreis von GINA-Web Fachpersonen des Forensisch-Psychiatrischen Dienstes der Universität Bern, externe Ärzt/innen zur somatisch-medizinischen Behandlung im Auftrag des AJV sowie mit dem Busseninkasso beschäftigtes Personal. Mit der Fachanwendung GINA-Web werden ca. 20–25 000 bernische Urteile inkl. Ersatzfreiheitsstrafen pro Jahr erfasst. Weiter werden der Vollzug von Strafen und Massnahmen an Erwachsenen und Jugendlichen im Umfang von circa 15 000 Dossiers sowie die Planung und Durchführung des Vollzugs in den entsprechenden Einrichtungen mit circa 400 000 Belegungstage pro Jahr verwaltet. Mit GINA-Web werden besonders schützenswerte Personendaten bearbeitet. Daraus resultiert ein erhöhter Schutzbedarf.

Im Fokus des Audits standen die nachweisbare und transparente Einhaltung der ISDS-Vorgaben, insbesondere in den Bereichen ISDS-Governance, -Konzepte und -Schutzmassnahmen, Prozesse des Benutzermanagements, Leistungsverträge mit wesentlichen Dienstleistern und weiteren Dritten (Outsourcing) sowie bei Schnittstellen der Fachanwendung als auch bei der Datenhaltung bzw. dem Daten-Life-Cycle.

Das Gesamtergebnis des Audits zeigte auf, dass wesentliche ISDS-Anforderungen noch nicht vollständig umgesetzt worden sind. Es wurden vorwiegend mittlere Risiken, insgesamt und als Fazit aber ein hohes Risiko für die Informationssicherheit und den Datenschutz festgestellt. Ausgehend vom Gesamtfazit ergaben sich dringende Handlungsempfehlungen, um die Datenschutz- und Sicherheitsvorgaben zeitnah einhalten zu können. Das AJV nahm sich den Handlungsempfehlungen und den daraus resultierenden ISDS-Aufgaben mit hoher Priorität an. Der Audit konnte in einem freundlichen und einsichtigen Umfeld durchgeführt werden.

Zentrale Restaurant- und Event-Datenbank

Zu den vom Bund angeordneten Massnahmen zur Bekämpfung der Covid-19-Epidemie gehörte die Erhebung von Kontaktdaten der Gäste von öffentlich zugänglichen Einrichtungen, Betriebe und Veranstaltungen. Aus den früher erwähnten Gründen (siehe dazu Ziff. 6.1.1) startete das Gesundheitsamt (GA) ein Projekt, welches die notwendigen Voraussetzungen zur systematischen und datenbankbasierenden zentralen Sammlung von Besuchs- bzw. Kontaktdaten schaffen sollten. Die Anzahl der potentiell von der Massnahme

betroffenen Personen wurde mit ca. 1 Million beziffert. Bei der entwickelten Zentralen Restaurant- und Event-Datenbank (ZRDB) handelt es sich um ein Datenbanksystem, das vom GA für die Bearbeitung von Besuchs- und Kontaktdaten von natürlichen Personen im Kanton Bern eingesetzt wird.

Im Rahmen des Audits wurde die nachweisbare Einhaltung der ISDS-Vorschriften im Umgang mit der zentralen Bearbeitung der Personendaten geprüft. Die Prüfgebiete umfassten dabei die ISDS-Governance, ISDS-Konzepte und umgesetzte Schutzmassnahmen, Prozesse des Datenbankbetriebs sowie das Zugangs- und Zugriffsmanagement, Leistungen Dritter einschliesslich Vertragsvereinbarungen als auch die eigentliche Datenhaltung und der Daten-Life-Cycle. Die für die betriebliche Bearbeitung der Personendaten verwendete Fachanwendung TRACY wurde eingeschränkt miteinbezogen (Einsichtnahme in ein praktisches Beispiel der Datenbearbeitung).

In allen Prüfgebieten wurden Defizite mit mittlerem Risiko für die betroffenen Personen erkannt und entsprechende Handlungsempfehlungen festgehalten. Insbesondere der Nachweis der regulatorisch klar festgelegten Löschung von nicht mehr benötigten Personendaten konnte nicht vollständig transparent erbracht werden. Weiter sind Fragen über die Datenqualität entstanden. Das GA bzw. das Generalsekretariat GSI hat sich den Handlungsempfehlungen angenommen. Der Audit konnte in einem freundlichen Umfeld durchgeführt werden.

«Therefore»

Die Pädagogische Hochschule Bern (PHBern) ist die Ausbildungsstätte für Lehrerinnen und Lehrer im Kanton Bern. Die Standorte für die Grundausbildung, Weiterbildung und Medienbildung sowie Forschung, Entwicklung und Evaluation befinden sich in der Stadt Bern. Die Beratungsstellen der PHBern sind über den Kanton verteilt. Für die Verwaltung der Studierendendaten wie Personenstammdaten, Leistungsnachweise und elektronische Dossier setzt die PHBern zwei Fachanwendungen ein: Omnitracker für die Verwaltung und Dokumentation der Studierendendaten und seit 2014 Therefore für die elektronische Archivierung der Studierendendossiers. Die PHBern betreibt Therefore in eigener Verantwortung auf ihrem Areal in Bern.

Im Fokus des Audits standen die Einhaltung der ISDS-Vorgaben bei der Bearbeitung von Personendaten mit Therefore. Dazu wurden die diesbezügliche Governance, Konzepte und Schutzmassnahmen, die Prozesse des Betriebs, das Identity and Access Management und die Leistungsverträge mit Dritten geprüft.

Bei der Prüfung wurden in allen geprüften Bereichen Verbesserungs- und Optimierungsmöglichkeiten festgestellt, welche mit einem mittleren und im Prüfgebiet ISDS-Governance mit einem höheren Risiko eingestuft wurden. Insbesondere konnte die DSA nicht erkennen, dass auf der Leitungsebene der

PHBern die ISDS-Anforderungen durch eine festgehaltene ISDS-Politik mit entsprechenden Zielen und Massnahmen sowie einem operativen ISDS-Rahmenwerk nachweisbar unterstützt wurden. Die Hauptlast liegt bei den IT-Verantwortlichen. Eine fehlende ISDS-Governance stellt auch im Zusammenhang mit der verabschiedeten PHBern-Digitalisierungsstrategie ein erhöhtes Risiko für die betroffenen Personen dar. Der Audit konnte in einem freundlichen und spürbar einsichtigen Umfeld durchgeführt werden.

Spitäler Frutigen Meiringen Interlaken AG

Die Spitäler Frutigen Meiringen Interlaken AG (fmi AG) sorgen für die medizinische Versorgung im Einzugsgebiet vom Frutigland bis zu den grossen Alpenpässen im Oberhasli. Das Diensstleistungsangebot der beiden Akutspitäler Interlaken und Frutigen umfasst die Schwerpunkte Chirurgie, Orthopädie/Traumatologie, Innere Medizin und Gynäkologie/Geburtshilfe. Im Gesundheitszentrum Meiringen hat die fmi AG einen 24-Stunden-Rettungsdienst stationiert. Zur fmi AG gehören auch das Pflegeheim Frutigland in Frutigen und Aeschi sowie der Seniorenpark Weissenau in Unterseen. Die fmi AG beschäftigt rund 1500 Mitarbeitende.

Im einem Prüfbericht von 2016 wurden im Rahmen des durchgeführten ISDS-Audits insgesamt 27 Handlungsempfehlungen festgehalten. Zwischen 2017 und 2020 wurde der Fortschritt der Umsetzung von ISDS-Massnahmen durch die DSA periodisch formal mit der fmi AG abgesprochen. Das Ziel des Nachaudits im 2021 umfasste in der Folge die nachweisbare Prüfung der erfolgreichen Umsetzung von ISDS-Massnahmen.

Das Gesamtergebnis des Nachaudits zeigte auf, dass von den 27 ISDS-Handlungsempfehlungen 16 erfolgreich umgesetzt wurden. 10 Empfehlungen wurden teilweise und eine Empfehlung noch nicht umgesetzt. Dies zeigt einmal mehr auf, dass die Umsetzung von ISDS-Verbesserungsmassnahmen eine grosse Herausforderung für die Beteiligten darstellt, insbesondere wenn die Empfehlungen grundlegende ISDS-Aspekte betreffen, welche unterschiedliche Funktionen und Dritte sowie die verantwortliche Leitungsebene adressieren. Im Rahmen der Schlussbesprechung zum Nachaudit wurden ISDS-Massnahmen kontrovers diskutiert. Die DSA musste einmal mehr feststellen, dass Verantwortliche noch nicht vollständig verstanden haben, dass es sich bei den ISDS-Anforderungen um gesetzliche Vorgaben handelt, welche zum Schutz der betroffenen Personen verbindlich einzuhalten sind. Der Audit konnte insgesamt in einem freundlichen und professionellen Umfeld durchgeführt werden.

Spital Insel Gruppe AG

Im Jahr 2016 fusionierte das Inselspital mit der Spital Netz Bern AG zur Insel Gruppe AG. Dadurch entstand das grösste medizinische Versorgungssystem der

Schweiz. In der Insel Gruppe werden jährlich über 800 000 Patient/innen behandelt und es werden über 10 000 Mitarbeitende beschäftigt. Die Direktion Technologie und Innovation (DTI) ist für das Technologiemanagement der Informations- und Kommunikationstechnologie (ICT) sowie der Medizintechnik verantwortlich; in der DTI arbeiten etwa 200 Mitarbeitende. Organisatorisch wurde die DTI neu aufgestellt und erhielt eine separate Abteilung «Governance, Risk & Compliance» (GRC), um insbesondere die ISDS-Risiken für die ICT und für die Medizintechnik von einer Stelle ausserhalb der operativen Teams besser kontrollieren und behandeln zu können.

Ein Audit der DSA im Jahr 2018 war sowohl bei der Durchführung als auch bei den erkannten Defiziten nicht ideal ausgefallen. In der Folge hatte die DSA mit den Verantwortlichen eine kontinuierliche und enge Begleitung der Umsetzung von ISDS-Massnahmen vereinbart. Aufgrund grosser organisatorischer und personeller Veränderungen bei der Insel Gruppe war die Umsetzung der ISDS-Verbesserungsmassahmen zunächst nicht zufriedenstellend verlaufen. Dies veranlasste die DSA, im 2021 einen weiter gefassten ISDS-Audit durchzuführen. Dieser umfasste dabei primär den sog. ICT-Grundschutz, d.h. alle Verfahren, Massnahmen, Organisation, Prozesse, Hilfsmittel, Infrastruktur und technische Systeme, Daten und Vorkehrungen etc., welche die sichere und datenschutzkonforme Abwicklung der Geschäftsprozesse (Datenbearbeitung) unterstützen. Bei der Prüfung stehen die konsequente und transparente sowie nachweisbare Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit sowie Authentizität der zu bearbeitenden Personendaten im Vordergrund.

Insgesamt konnte festgestellt werden, dass die Insel Gruppe im letzten Jahr grundlegende und richtige Massnahmen ergriffen hat, um die Informationssicherheit und den Datenschutz grundsätzlich zu verbessern. Dazu gehören namentlich die Etablierung der vom operativen Betrieb unabhängigen Abteilung GRC innerhalb der DTI, der noch laufende Aufbau eines Informationssicherheits-Managementsystems sowie die Umsetzung zentraler Prozesse. Die Gesamtsituation beurteilt die DSA derzeit immer noch als solche mit einem hohen, kaum zu akzeptierenden ISDS-Risiko, und es müssen noch wesentliche Verbesserungen umgesetzt werden, damit die Risiken durch die zum Teil bereits konzipierten Massnahmen weiter gesenkt werden können. Insbesondere bestehen für die gesamte Insel Gruppe noch keine verbindlichen direktionsübergreifenden ISDS-Vorgaben und -Massnahmen. Der durchgeführte Audit erfolgte in einem professionellen und freundlichem sowie konstruktiven Umfeld.

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 übergab die DSA der Projektleitung der DIJ zuhanden der Revision des KDSG das Ergebnispapier der informellen Arbeitsgruppe bestehend aus einer Vertretung des Verbands Bernische Gemeinden, des AGR, der Regierungsstatthalterämter und der DSA. Das im Vorjahr anlässlich eines Workshops mit Vertreter/innen unterschiedlich grosser Gemeinden besprochene Arbeitspapier enthält Grundlagen für mögliche Varianten der künftigen Organisation der Datenschutzaufsicht für die Gemeinden gemäss dem bernischen Gemeindegesetz. Als Teil des ordentlichen Gesetzgebungsprozesses sollen die Vorschläge breit diskutiert werden können.

Beratung zu kommunalen Videoüberwachungen

Im Rahmen ihrer Oberaufsicht beriet die DSA mehrere kommunale Aufsichtsstellen zum Thema Videoüberwachungen in den Gemeinen. Bei der Videoüberwachung für eine Schulanlage ging es um das ordnungsgemässe Vorgehen nach dem Polizeigesetz und dem KDSG sowie um Inhalt und Form der Stellungnahme, welche die kommunale Aufsichtsstelle zuhanden der KAPO erarbeiten musste.

Zudem waren Fragen einer besorgten Privatperson zu beantworten. In einem anderen Fall ging es um eine private Videoüberwachung, welche auch einen öffentlich genutzten Durchgangsweg erfasste. Hier erkundigte sich ein Gemeindemitarbeiter, mit welchen Mitteln die Gemeinde gegen die private Überwachung des öffentlichen Bereichs vorgehen könne.

6.7 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, wovon eine auf dem Zirkularweg und eine als Präsenzveranstaltung. Mit der dabei erfolgten Aufnahme des Datenschutzbeauftragten der Kantone Schwyz, Obwalden und Nidwalden sind nun wieder alle kantonalen Datenschutzbehörden Mitglieder von privatim. Der Vorstand und dessen Ausschuss verfassten zu 13 Vernehmlassungen oder Konsultationen des Bundes Stellungnahmen von privatim und teils zusätzlich Mustervorlagen für die Mitglieder. Im Austausch mit dem EDÖB wurden Themen wie die Auswirkungen des «Schrems II»-Urteils des Europäischen Gerichtshofs, die systematische Verwendung der AHV-Nummer sowie materielle und Zuständigkeitsfragen im Rahmen der Pandemie besprochen. Zudem pflegte privatim den Kontakt zur SIK, zur neuen Organisation «Digitale Verwaltung Schweiz», zu den Institutionen Educa und SWITCH im Bereich der Bildung- und Forschung sowie zur eOperations AG, wo sich privatim für datenschutzkonforme Dienstleistungsverträge der Kantone einsetzte.

Arbeitsgruppen von privatim

Die *Arbeitsgruppe Digitale Verwaltung* und eine dafür eingesetzte Unterarbeitsgruppe befassten sich mit dem Gutachten «Once Only und das Rechtsstaatsprinzip», welches Prof. Astrid Epiney und ihre Assistentin Sophia Rovelli verfasst hatten. Die Unterarbeitsgruppe erarbeite ein Begleitdokument für die privatim-Mitglieder, welches zusammen mit der Publikation verteilt werden soll. Dabei erwies sich das bernische PDSG als gutes Beispiel für eine mögliche datenschutzkonforme Lösung.

Die *Arbeitsgruppe Sicherheit* traf sich zu einer virtuellen und einer physischen Arbeitssitzung, um gemeinsam Fragen zur polizeilichen Überwachung mit technischen Hilfsmitteln, zum interkantonalen Datenaustausch im Polizeibereich und zu weiteren Datenschutzaspekten im Polizei- und Justizwesen zu erörtern.

Ausserdem wohnten mehrere Mitglieder der Arbeitsgruppe einem Informationsanlass bei, den die Projektleitung des Vorhabens «Integriertes Lagebild 4.0» organisierte, um die Datenschutzbehörden der am Projekt beteiligten Kantone frühzeitig einzubeziehen und deren Anforderungen berücksichtigen zu können.

Unter der Leitung der stellvertretenden Datenschutzbeauftragten fanden im Berichtsjahr sieben virtuelle Sitzungen der Arbeitsgruppe Gesundheit statt. Der Austausch unter den auf den Datenschutz im Gesundheitswesen spezialisierten Mitgliedern fokussierte sich erneut auf wichtige datenschutzrechtliche Fragestellungen während der Pandemie. Die Abklärungen und Erfahrungen des Kantons Bern betreffend die zentrale Kontaktdatenbank und die VacMe-Plattform boten den anderen kantonalen Datenschutzbehörden interessante Hinweise. Umgekehrt erhielt der Kanton Bern wichtige Inputs bezüglich Impfdokumentation und Impfregister (rechtliche Einordnung und Verantwortlichkeit, auch mit Blick auf die Aufbewahrung). Ausserhalb der Pandemie-Themen wurde der Austausch über die Einführung des Elektronischen Patientendossiers wiederaufgenommen, er soll im Folgejahr weiter intensiviert werden.

In der *Arbeitsgruppe ICT* tauschten sich Vertreter/innen von Kantonen, deren Aufsichtsstellen über Informationssicherheitsspezialisten verfügen, über aktuelle technische Fragen aus.

7 Antrag

Kenntnisnahme.

8 Glossar / Abkürzungen

ABEV	Amt für Bevölkerungsdienste
AGR	Amt für Gemeinden und Raumordnung
AJV	Amt für Justizvollzug
ArchG	Gesetz über die Archivierung (Archivgesetz)
ASV	Amt für Sozialversicherungen
BAG	Bundesamt für Gesundheit
BKD	Bildungs- und Kulturdirektion
DIJ	Direktion für Inneres und Justiz
DSA	Datenschutzaufsichtsstelle des Kantons Bern
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
DTI	Direktion Technologie und Innovation des Inselspitals
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EpG	Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz)
EU	Europäische Union
FIN	Finanzdirektion
FK	Finanzkontrolle
fmi AG	Spitäler Frutigen Meringen Interlaken AG
GA	Gesundheitsamt
GERES V	Verordnung über die Gemeinderegistersysteme-Plattform
GRC	Abteilung Governance, Risk & Compliance des Inselspitals
GSI	Gesundheits-, Sozial- und Integrationsdirektion
ICT	Informations- und Telekommunikationstechnik
IPv6	Internet Protokoll Version 6

ISDS	Informationssicherheit und Datenschutz
IT	Informatik
KAIO	Kantonales Amt für Informatik und Organisation
KAPO	Kantonspolizei
KDSG	(Kantonales) Datenschutzgesetz
KRBESO	Krebsregister Bern Solothurn
KRG	Bundesgesetz über die Registrierung von Krebserkrankungen (Krebsregistrie-rungsgesetz)
LAN	Local Area Network
PDSG	Gesetz über die zentralen Personendatensammlungen (Personendatensammlungsgesetz)
PHBern	Pädagogische Hochschule Bern
PolG	Polizeigesetz
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
RSW	Registrierungssoftware
SDK	Service Desk
SIK	Schweizerische Informatikkonferenz
STA	Staatskanzlei
StAB	Staatsarchiv
WEU	Wirtschafts-, Energie- und Umweltdirektion
TCHF	Tausend Franken
USA	Vereinigte Staaten von Amerika
VGE	Verwaltungsgerichtsentscheid
WAN	Wide Area Network
ZRDB	Zentrale Restaurant- und Event-Datenbank

Datenschutzaufsichtsstelle
des Kantons Bern

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

www.be.ch/dsa