Kanton Bern
Canton de Berne

Jahresbericht Datenschutzaufsichtsstelle 2019

Datenschutzaufsichtsstelle

Februar 2020

Impressum

Herausgeber:
Datenschutzaufsichtsstelle
des Kantons Bern

Layout und Realisation: noord.ch


Y
U
J
N
G

1 Vorwort

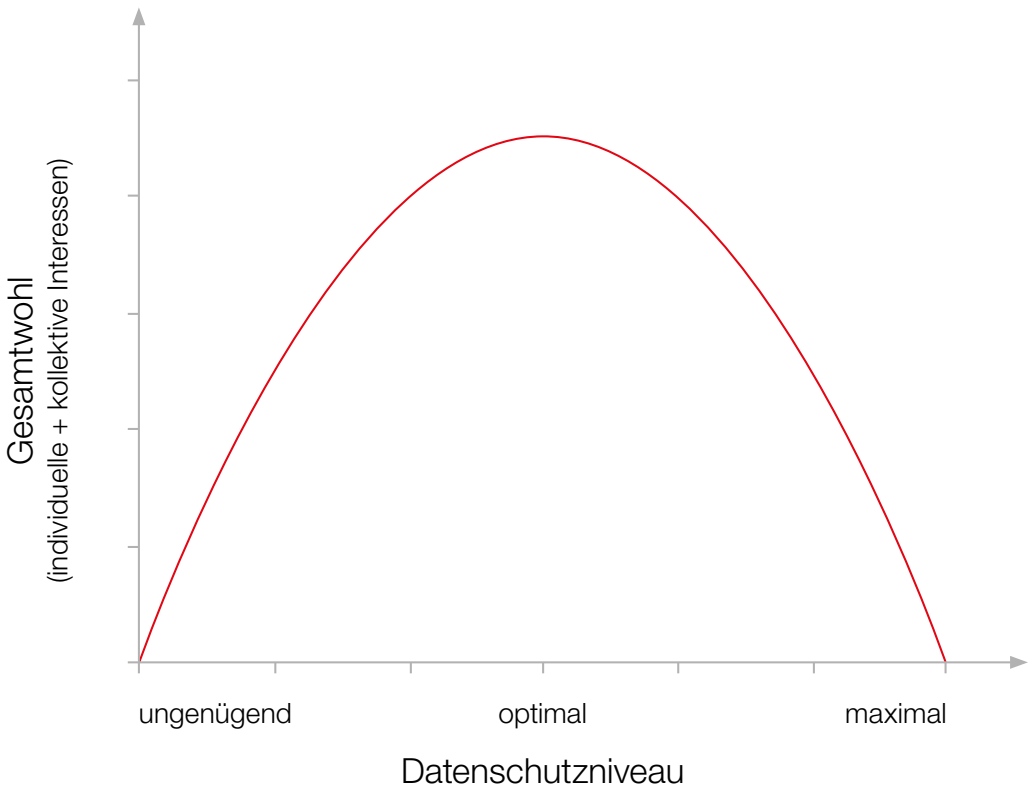
Nachdem der Regierungsrat in seinen am 8. Januar 2019 verabschiedeten Regierungsrichtlinien 2019–2022 angekündigt hatte, die digitale Transformation der Verwaltung mit einer direktionsübergreifenden Strategie vorantreiben und das digitale Primat im Verkehr zwischen Staat und Privaten bzw. Unternehmen sowie zwischen Behörden umsetzen zu wollen, genehmigte er am 26. Juni 2019 die «Strategie Digitale Verwaltung des Kantons Bern 2019–2022». Als erste zentrale Anforderung an «gute» elektronische Dienstleistungen von Behörden nennt er darin das Vertrauen – insbesondere in Persönlichkeits- und Datenschutz sowie Datensicherheit – als elementare Voraussetzung, damit Bevölkerung und Wirtschaft digitale Services nutzen. Nebst seiner grundlegenden Aufgabe als ein tragendes Element jeder rechtsstaatlichen Demokratie ist der Datenschutz also auch ein Qualitätsmerkmal und letztlich «Verkaufsargument» für elektronischen Behördenverkehr.

Auch die Datenschutzaufsichtsstelle (DSA), welche im Frühjahr 2019 infolge zweier Pensionierungen und eines weiteren Austritts personell zur Hälfte erneuert wurde, hat im Berichtsjahr eine Strategie formuliert. Zu den strategischen Zielen gehört die Sicherstellung eines optimalen Datenschutzniveaus (siehe dazu Ziff. 2 unten) in Gesetzgebung und Verwaltungstätigkeit auf allen Ebenen des Kantons Bern, die Stärkung der bei den Behörden vorhandenen Kompetenzen im Bereich Datenschutz und Informationssicherheit sowie die Schärfung des Profils der DSA als unabhängige Anlaufstelle für Direktionen und Ämter, welche sich bei der Wahrnehmung ihrer Datenschutzverantwortung fachlich beraten und unterstützen lassen wollen (unten Ziff. 6 Bst. a). Der frühe Einbezug in datenschutzrelevante Gesetzgebungsvorhaben (Bst. b) oder Informatikprojekte (Bst. c) erlaubt der DSA eine präventive Form der Aufsicht, welche zu einer Verlagerung von der Frage, *ob* eine Bearbeitung von Personendaten zulässig ist, hin zur Frage führt, *wie* eine Datenbearbeitung rechtskonform erfolgen kann. Das gleiche Ziel verfolgen auch die Sicherheitsprüfungen von produktiven IT-Systemen und -Applikationen (Bst. d), welche den geprüften Stellen Hinweise geben, in welchen Bereichen sie das Schutzniveau weiter erhöhen können. Letztlich geht es darum, dass der Datenschutz für alle mit Personendaten befassten Behörden – und das dürften sämtliche Behörden sein – zur Selbstverständlichkeit wird. Dann verdienen sie das Vertrauen der Bevölkerung, welche ihre digitalen Services nutzen soll.

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. 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.

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 2019 verfügte die DSA über einen Personalbestand von 500 % (bei einem bewilligten Bestand von 515 %), aufgeteilt auf sechs Personen. Davon sind vier 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 rund 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 in datenschutzrechtlichen Fragen. In Vorabkontrollen prüft sie die eingereichten ISDS-Dokumente hinsichtlich rechtlicher Aspekte.

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

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 2019 betrug der Betriebsaufwand der DSA insgesamt TCHF 202 (Budget: TCHF 227). Davon wurde der weit überwiegende Teil (TCHF 160) für externe Dienstleistungen zur Unterstützung von Informatikprüfungen eingesetzt.

Innerhalb der kantonalen Verwaltung bestehen weitere Anlaufstellen, welche die verantwortlichen Behörden in ISDS-Fragen beraten: So verfügen die Direktionen und die 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 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 auch institutionalisierte Kontakte zu Behörden, bei deren Tätigkeiten sich regelmässig anspruchsvolle datenschutzrechtliche Fragen stellen (Beispiele: Kantonales Amt für Informatik und Organisation [KAIO], Bedag AG und Insel Gruppe AG).

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) von privatim, in allen fachbezogenen Arbeitsgruppen (zurzeit Digitale Verwaltung, Sicherheit und ICT) nimmt eine Person der DSA teil, und die DSA hat die Initiative ergriffen, um auch die Arbeitsgruppe Gesundheit weiterzuführen.

6 Fachliche Berichterstattung «aus dem Arbeitsalltag»

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

6.1 Beratung

6.1.1 Behörden

Publikation von Eigentümeradressen im Internet

Als öffentliches Register soll das Grundbuch Publizität über die Eigentumsverhältnisse schaffen und eine Identifikation der Eigentümer erlauben. Das Grundbuchrecht des Bundes sieht zwar vor, dass zur Bezeichnung der Eigentümerschaft Namen, Geburtsdatum und Heimatort bekannt gegeben werden dürfen, die Adresse ist jedoch nicht erwähnt. Dies dürfte damit zusammenhängen, dass es keine Pflicht zur Aktualisierung des Grundbuchs gibt. Im Kanton Bern wird die Adresse aus der Zentralen Personenverwaltung (ZPV) bezogen und damit laufend aktualisiert, was die Aussagekraft des Grundbuchs als öffentliches Register erhöht. Jedoch erlaubt dies auch grundbuchfremde Erkenntnisse, z.B., dass einer von zwei Miteigentümern aus dem Eigenheim ausgezogen ist. Im Falle einer Publikation der Eigentümeradressen im Internet muss es deshalb möglich und technisch umsetzbar sein, dass Personen mit schutzwürdigen Interessen die Bekanntgabe ihrer Adresse sperren lassen können.

Zugriffe auf Dossiers im Bereich Kindes- und Erwachsenenschutz

Ein früheres Audit bei der Kindes- und Erwachsenenschutzbehörde (KESB) hatte ergeben, dass in der elektronischen Geschäftsverwaltung (GEVER) der KESB alle Behördenmitglieder und Mitarbeitenden Zugriff auf alle Dossiers aller 11 regionalen Standorte hatten, was weit über das für die Aufgabenerfüllung erforderliche Mass hinausging. Eine neue Version des GEVER-Systems erlaubt nun eine differenziertere Vergabe der Berechtigungen, so dass der Zugriff grundsätzlich auf die Dossiers der eigenen Region eingeschränkt werden kann. Für Behördenmitglieder mit regionsübergreifenden Pikettdiensten, ausgewählte Kanzleimitarbeitende und das Sekretariat der Geschäftsleitung, welche bei Bedarf weiterhin auf Dossiers aus alle Regionen zugreifen können müssen, sollen ein Loggen der Zugriffe und stichprobeweise Kontrollen sicherstellen, dass Zugriffe weisungsgemäss nur dann erfolgen, wenn es für einen konkreten Arbeitsschritt unentbehrlich ist.

Verlorener USB-Stick

Artikel 8 der seit September 2018 geltenden Einführungsverordnung zur EU-Datenschutzrichtlinie (EV EDS) sieht für Behörden im Strafbereich die Pflicht vor, Verletzungen des Datenschutzes der DSA zu melden (sog. «Data Breach Notification»). Dass auch Behörden, die der EV EDS nicht unterstehen, die Problematik von Datenschutzverletzungen ernst nehmen, zeigt der Fall einer freiwilligen Verletzungsmeldung einer kantonalen Behörde aus dem Gesundheitswesen. Die Behörde hatte der Finanzkontrolle (FK) im Rahmen einer Revision per Briefpost einen USB-Stick zugeschickt, auf dem u.a. unverschlüsselte Personendaten mit besonderer Geheimhaltungspflicht gespeichert waren. Der USB-Stick wurde mutmasslich von einem Dritten mit einem Messer aus dem Briefumschlag entfernt, bevor die FK die Sendung aus ihrem Postfach entnehmen konnte. Die freiwillige Meldung der Behörde wird von der DSA als sehr positiv bewertet, und die selbstbewusste Fehlerkultur der Behörde darf als Musterbeispiel gelten. Die bevorstehende Revision des KDSG wird eine generelle Pflicht zur Meldung von Datenschutzverletzungen schaffen. Die DSA nimmt auch weiterhin freiwillige Meldungen von Behörden entgegen, welche nicht der EV EDS unterstehen.

Herausgabe von Randdaten einer Lehrperson an die Anstellungsbehörde

Eine Anstellungsbehörde wollte die bei der Nutzung von Microsoft Office 365 in Heimarbeit angefallenen Randdaten – d.h. Daten über das Nutzerverhalten (z.B. wer hat welche Anwendung in welchem Zeitraum benutzt) – einer bestimmten Lehrperson erfahren, um die Korrektheit der Arbeitszeitverbuchung zu überprüfen. Gestützt auf die Personalverordnung hielt die DSA die Voraussetzungen für das Bearbeiten der Randdaten wie folgt fest: Es muss ein genügend verdichteter Verdacht eines Missbrauchs vorliegen und die Überwachung muss vorgängig angekündigt worden sein. Seit dem 1. Januar 2020 sind die Aufzeichnung und Auswertung von Randdaten in der Randdatenverordnung kantonsweit verbindlich geregelt (siehe unten Ziff. 6 Bst. b).

Übergabe von Personendaten an eine Landeskirche

Seit dem 1. Januar 2020 sind die Landeskirchen gestützt auf das neue Landeskirchengesetz (LKG) selbständig zuständig für ihr Personal. Bis anhin wurde diese Arbeit vom Beauftragten für kirchliche Angelegenheiten des Kantons (heute: Beauftragter für kirchliche und religiöse Angelegenheiten) geleistet. Das LKG regelt auch den Übergang der Arbeitsverhältnisse, gilt aber erst ab 2020. Deshalb stellte sich die Frage, zu welchem früheren Zeitpunkt der reformierten Landeskirche die Personaldaten übergegeben werden dürfen. Die DSA kam zum Schluss, dass die Landeskirche ein Anrecht hat, die Daten der künftig weiterhin angestellten Pfarrpersonen einige Monate vor dem Inkrafttreten des neuen Gesetzes

zu erhalten, damit sie die Lohnzahlungen und weiteren personalrechtlichen Ansprüche rechtzeitig vorbereiten kann.

Forschungsprojekt Häusliche Gewalt

Die Berner Interventionsstelle gegen häusliche Gewalt der Polizei- und Militärdirektion (heute: Sicherheitsdirektion) bat die DSA, den Start zu einem Forschungsprojekt zu häuslicher Gewalt zu begleiten, an dem Behörden zweier Kantone sowie private Vereine mitwirken werden. Im Projekt werden sensible, besonders schützenswerte und durch Schweigepflichten geschützte Daten bearbeitet. Der Datenschutz sollte deshalb von Anfang an angemessen berücksichtigt werden. Mit Hilfe einer tabellarischen Übersicht konnten sich die Teilnehmenden Klarheit über ihre datenschutzrechtlichen Pflichten verschaffen.

6.1.2 Betroffene Personen

Vermittlung betreffend Akteneinsicht bei der Kantonspolizei (KAPO)

Ein Bürger fand bei einer gewährten Akteneinsicht nicht alle erwarteten Informationen vor und gelangte deshalb an die DSA. Diese konnte vermittelnd klären, dass das mobile Abfragesystem der KAPO keine zusätzlichen Daten enthält, die dem Bürger nicht gezeigt wurden. Bei der erwarteten Angabe, dass bei allen Angelegenheiten betreffend eine bestimmte Person die gleiche Ansprechperson der KAPO zu kontaktieren sei, handelte es sich um eine polizeiinterne Dienstanweisung an die Beamten und nicht um Personendaten des Betroffenen, in welche Einsicht zu gewähren ist.

Abgabe von Adresslisten an Schützenvereine

Jugendliche erhalten regelmässig ungefragt Einladungen von Schützenvereinen. Die DSA wurde angefragt, ob die Gemeinden jenen Vereinen Adressen zur Verfügung stellen dürfen. Die Abklärungen ergaben, dass Jungschützenkurse als vordienstliche Ausbildung im Sinne der einschlägigen Verordnung des Bundes gelten. Die Gemeinden dürfen den Schützenvereinen deshalb die Adressen der 15- bis 20-Jährigen bekanntgeben.

Webseiten von Behörden

1. IP-Adressen in Online-Formularen
Eine betroffene Person fragte die DSA an, ob die Erhebung ihrer IP-Adresse bei Benützung eines Online-Kontaktformulars der KAPO rechtmässig sei.

Die Verantwortung für die inhaltliche Ausgestaltung und die korrekte Konfiguration von Online-Formularen liegt bei der Behörde, welche ein Formular aufschaltet. Sie muss namentlich über eine genügende gesetzliche Grundlage verfügen, um die jeweiligen Daten beschaffen zu dürfen, was hier nicht klar war. Die DSA hielt die separate Erhebung der IP-Adresse für unnötig und empfahl der KAPO, künftig darauf zu verzichten. Die IP-Adressen, von welchen aus Online-Formulare abgeschickt werden, werden nämlich systembedingt bereits an einem zentralen Ort aufgezeichnet, während einer verhältnismässig kurzen Frist aufbewahrt und danach automatisch gelöscht. Weil die KAPO auch auf anderem Weg kontaktiert werden kann, verzichtete die DSA auf einen formellen begründeten Antrag.

2. Einsatz von Cookies
Die Website einer öffentlich-rechtlichen Anstalt enthielt eine Datenschutzerklärung mit Hinweisen auf den Einsatz von Cookies, der von den Besuchern nicht abgelehnt werden konnte. Im Gespräch mit den verantwortlichen Personen wurde geklärt, welche Cookies von Behörden eingesetzt werden dürfen (nämlich solche, die für den Betrieb notwendig sind) und welche nicht (solche, die bloss ein besseres Benutzererlebnis ermöglichen oder zu Marketingzwecken eingesetzt werden). Die betreffende Website wurde innert nützlicher Frist angepasst.

«Doppelgänger-Fall»

Eine besorgte Bürgerin meldete der DSA, dass ein mutmasslich in einem Berner Spital aufgenommenes Bild ihres verstorbenen Vaters im Internet aufgetaucht sei und dort zur Untermalung von Artikeln als sog. «Stock-Foto» verwendet werde. Nach Beratung durch die DSA und Abklärungen der Bürgerin stellte sich heraus, dass es sich bei der Person im Bild gar nicht um den Vater der Bürgerin handelte, sondern um jenen des Fotografen selbst. Die beiden Väter sahen einander derart ähnlich, dass sogar ihre Kinder sie auf den ersten Blick nicht voneinander unterscheiden konnten.

Digitalisierung an Volksschulen

Die Volksschulen werden von den Gemeinden geführt und unterstehen deshalb der Datenschutzaufsicht der Gemeinden bzw. der betreffenden Gemeindeverbände. Dennoch wird die kantonale DSA regelmässig mit Anliegen betreffend die Volksschulen kontaktiert. Namentlich die schwierigen Fragestellungen rund um den Einsatz des Google-Produkts «G Suite for Education» gemeinsam mit Google Chrome Books beschäftigen die kommunalen Behörden und auch die Eltern immer wieder. Mehrere direkt oder in Kopie an die DSA gerichtete Schreiben von besorgten Eltern wiesen darauf hin, dass diese die Geschäftsbedingungen von Google als kritisch erachten. Auf kantonaler Ebene laufen diverse Bestrebungen, um die Volksschulen datenschutzrechtlich zu unterstützen. So stellt z.B. die Pädagogische Hochschule Bern nebst anderen Hilfsmitteln und Beratungsleistungen ein Online-Tool zur Verfügung, mit welchem die Schulen

basierend auf einem Ampelsystem einen Flyer zur Sensibilisierung generieren können. Ebenfalls bemüht sich die DSA im Rahmen der Konferenz der schweizerischen Datenbeauftragten (privatim), via die Fachagentur educa.ch Rahmenverträge mit grossen Softwareanbietern zu erreichen, unter denen alle schweizerischen Bildungsinstitutionen datenschutzkonforme Vertragsbedingungen – namentlich die Anwendung von Schweizer Recht – erhalten.

Bekanntgabe der AHV-Nummer an alle Kursteilnehmer im Zivilschutz

Ein Zivilschutzdienst-Teilnehmer fragte die DSA an, ob das Bekanntgeben seiner AHV-Versichertennummer auf einer an alle Teilnehmer eines Dienstanlasses gesendeten Liste statthaft sei. Die Anfrage gab Anlass zu einer aufsichtsrechtlichen Rückfrage an die betroffene Zivilschutzstelle. Die DSA fragte nach der Rechtsgrundlage und dem Zweck der Bekanntgabe der Versichertennummer und zusätzlich der Berufsangabe und des Geburtsdatums. Gemäss Antwort der Behörde handelte es sich um eine versuchsweise und auf Wunsch der Teilnehmenden versendete Liste, die Verwendung der drei Datenkategorien wurde mit internen Abläufen begründet. Die DSA stellte fest, dass die Bekanntgabe der Daten über den Versuch hinaus rechtlich nicht abgestützt und deshalb unzulässig ist. Für die interne Aufgabenerfüllung bestehen hingegen ausreichende Rechtsgrundlagen für die Bearbeitung der drei Datenkategorien. Die DSA forderte die Zivilschutzbehörde auf, das Aufgebot für einen Zivilschutzeinsatz entsprechend anzupassen.

Schützt KDSG anonyme Anzeiger?

Eine Privatperson wollte wissen, ob das KDSG sie schütze, wenn sie im Fall einer Anzeige – hier bei der Polizei – anonym bleiben wolle. Die Antwort hängt davon ab, ob das Datenschutzgesetz überhaupt zur Anwendung gelangt. Dies ist nur dann der Fall, wenn mit der Anzeige kein Straf- oder Verwaltungsjustizverfahren eingeleitet wird; dann gelten die jeweiligen Verfahrensrechte. Gilt das KDSG, so schützt es einzig dann vor einer Einsichtnahme in die Unterlagen durch die angezeigte Person, wenn die anzeigende Person besonders schützenswerte Interessen geltend machen kann. Die Rechtsprechung stellt allerdings sehr hohe Anforderungen an das Vorliegen solcher Interessen: Es muss beispielsweise nachweislich eine konkrete Gefährdung der Integrität oder eine ernsthafte Verletzung der Persönlichkeit drohen. Das dürfte selten der Fall sein und bedeutet, dass Anzeigende in der Regel zu ihrer Anzeige stehen müssen.

6.2 Formelle Stellungnahmen

Personendatensammlungsgesetz (PDSG)

Das neue Gesetz soll eine Rechtsgrundlage dafür schaffen, dass Personendaten, die mehrere Behörden zur Erfüllung ihrer gesetzlichen Aufgaben benötigen und bearbeiten dürfen, in zentralen Personendatensammlungen bereitgestellt werden können. Auf solche Sammlungen dürfen einzig Behörden zugreifen, welche in ihrem Fachbereich eine genügende Rechtsgrundlage für die Datenbearbeitung aufweisen. Als Übergangslösung schafft der Anhang zum PDSG eine Vermutung, dass die für jedes Fachgesetz explizit erwähnten Datenkategorien zur Aufgabenerfüllung benötigt werden, mittelfristig sollen die Fachgesetze selbst entsprechend ergänzt werden (im Rahmen laufender Revisionen – z.B. des Notariatsgesetzes – werden die notwendigen Ergänzungen bereits aufgenommen). Während die Zugriffe auf das Gemeinderegistersystem GERES heute nach einem politischen Prozess vom Regierungsrat gewährt werden, sollen die Direktionen die in ihrem Fachbereich benötigten Berechtigungen künftig selbst festlegen können, was die Flexibilität erhöht; gleichzeitig ist jede neue Berechtigungsregelung der DSA zur Prüfung vorzulegen, welche erhebliche Differenzen bis vor das Verwaltungsgericht bringen kann, so dass eine rechtliche Prüfung der Zulässigkeit sichergestellt ist. Die DSA wurde vom federführenden KAIO eng in die Vorarbeiten einbezogen, so dass der vom Regierungsrat verabschiedete Gesetzesentwurf dem Datenschutz bestmöglich Rechnung trägt.

Randdatenverordnung (RDV)

Eine per 1. Januar 2020 in Kraft getretene Revision des Personalgesetzes enthält neue Vorschriften über die Bearbeitung von Randdaten, die bei der Nutzung der elektronischen Infrastruktur durch die Mitarbeitenden in der kantonalen Verwaltung anfallen. Diese Vorschriften werden in der neuen RDV konkretisiert. Die DSA wurde früh in die Arbeiten einbezogen und konnte der Verordnung im Ergebnis zustimmen. Die RDV lehnt sich zwar an Bundesrecht an, enthält aber punktuell Klärungen und strengere Regelungen, die dem Datenschutz des Kantonspersonals dienen. So sind nicht namentliche personenbezogene Auswertungen durch die Betreiberin oder die nach den ISDS-Vorschriften vorgesehenen Stellen nur im Auftrag oder mit Zustimmung der verantwortlichen Behörde zulässig. Ausserdem dürfen solche Auswertungen nur stichprobeweise erfolgen. Der Vortrag enthält klare Erläuterungen und Hinweise für eine datenschutzkonforme Anwendung der RDV.

eUmzug (Abschluss 1. Phase)

Bei eUmzug handelt es sich um ein Versuchsprojekt des Kantons Bern, welches Bürgerinnen und Bürgern ermöglichen soll, online und ohne Gang an den

Schalter einen Wohnortwechsel vorzunehmen. Das Amt für Gemeinden und Raumordnung gab die zweite Phase des eUmzug-Versuchs am 23. September 2019 frei und schloss damit gleichzeitig die erste Phase ab. Die Stellungnahme der DSA zur ersten Phase wurde im Rahmen der Phasenfreigabe vollumfänglich berücksichtigt. In einem nächsten Schritt wird eine Prüfung der Informationssicherheit von eUmzug durch eine externe Leistungserbringerin durchgeführt. Die DSA steht mit den Datenschutzaufsichtsstellen anderer Kantone diesbezüglich in Kontakt, da eUmzug schweizweit im (testweisen oder produktiven) Betrieb ist und somit eine Koordination unter den Aufsichtsstellen notwendig macht.

Revision Volksschulgesetz 2020

Die DSA wurde bei der Vorbereitung des Vernehmlassungsentwurfs zur Mitwirkung eingeladen. In ihrem Mitbericht hielt die DSA fest, dass die vorgesehene Rechtsgrundlage für die Datenbekanntgabe im Rahmen der Abklärung des sonderpädagogischen Bedarfs von Kindern und Jugendlichen nicht ausreiche, weil die betroffenen Personendaten besonders schützenswert sind. Die Bemerkungen wurden ohne überzeugende Begründung nicht berücksichtigt. Die DSA liess sich deshalb im Rahmen der Vernehmlassung selbst nochmals und mit Nachdruck vernehmen.

Einführungsverordnung zur eidgenössischen Krebsregistrierungsgesetzgebung (EV KRG)

Per 1.1.2020 sind das Krebsregistrierungsgesetz des Bundes und die zugehörige Verordnung in Kraft getreten. Die DSA regte im Mitberichtsverfahren zur kantonalen EV KRG an, weitere datenschutzrechtliche und -technische Minimalinhalte in den Katalog des Leistungsvertrags zwischen dem Kantonsarztamt und der Krebsregistrierungsstelle aufzunehmen. Die Aufnahme von ISDS-Regelungen und die Pflicht zur Datenübergabe an die neue kantonale Registrierungsstelle bei einer Vertragsbeendigung wurden von der zuständigen Gesundheits- und Fürsorgedirektion (GEF; heute: GSI) übernommen. Demgegenüber wurde eine Verpflichtung zur Datenlöschung nach einer Übergabe der Daten an eine neue Krebsregistrierungsstelle als überflüssig taxiert. Weil die Übergabe von elektronischen Daten nicht automatisch bedeutet, dass die abgebende Stelle selbst nicht mehr über die Daten verfügt, wäre eine ausdrückliche Regelung wünschbar gewesen. Immerhin bleibt die allgemeine Regelung des KDSG anwendbar, wonach nicht mehr benötigte Daten zu löschen sind. Mit dem Übergang des Bearbeitungsrechts auf die neue Stelle verliert die bisherige ihr Recht, so dass die Daten bei der alten Stelle zu löschen sind.

Revision Spitalversorgungsgesetz (SpVG)

Im Fokus des Mitberichts der DSA zur Revision des SpVG lag eine Bestimmung zur Datenlieferung. Die Listenspitäler müssen administrative und neu auch medizinische Daten für die vom Kanton mitfinanzierten Leistungen in nicht anonymisierter Form abliefern, soweit dies zur wirksamen Rechnungskontrolle erforderlich ist. Weil diese Kontrolle in der Vergangenheit gestützt auf eine tarifvertragliche Abmachung durch die Krankenversicherer und nicht durch den Kanton erfolgte, erschien der DSA die Datenschutzkonformität des neuen Vorgehens als zweifelhaft. Sie bot der GEF (heute: GSI) eine gemeinsame Klärung der offenen Frage an, worauf ein konstruktiver Austausch stattfand mit dem Ergebnis, dass eine konsolidierte Fassung der Vorlage in die Vernehmlassung gegeben werden konnte.

Bundesvernehmlassung zur Änderung des DNA-Profil-Gesetzes

Neu will der Bund die sogenannte Phänotypisierung erlauben, d.h. die Feststellung äusserlicher Merkmale (z.B. Augen-, natürliche Haar- oder Hautfarbe) eines Spurengebers aus DNA-Material, welches an einem Tatort sichergestellt wurde. Im Entwurf für eine Stellungnahme des Kantons Bern wollte die Polizei- und Militärdirektion (POM; heute: Sicherheitsdirektion) die zulässige Analyse auch auf andere als äusserliche Merkmale (z.B. angeborene Farbenblindheit) ausdehnen. Die DSA lehnte eine solche Ausdehnung ab, weil dies den Eingriff in die Rechte der Personen, die auf eine Übereinstimmung mit den Analyseergebnissen hin überprüft werden, erheblich erhöhen würde; jene Personen müssten nämlich Einblick in Angaben zu ihrem körperlichen Zustand gewähren, welche zu den besonders schutzwürdigen Angaben gehören. Leider hat der Regierungsrat die Einwände der DSA nicht gehört und die Stellungnahme im Sinne der POM verabschiedet.

6.3 Vorabkontrollen

6.3.1 Informatikprojekte

Der DSA zur Vorabkontrolle zu unterbreiten sind geplante – regelmässig 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 113 Vorabkontrollen (Vorjahr: 71) zu Informatikprojekten bearbeitet und dabei 69 (28) bzw. 61.06 % (39.44 %) abgeschlossen. Seit dem Frühjahr 2019 werden diese 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.

Elektronische Geschäftsverwaltung (GEVER): Mandanten der Direktionen und Ämter

Das für alle Mandanten gültige ISDS-Konzept «BE-GEVER Konzern» war insoweit ein untypischer Vorabkontroll-Gegenstand, als zunächst lediglich eine Applikation einschliesslich der Möglichkeiten zur spezifischen Konfiguration beschrieben wurde und nicht ihr Einsatz für konkrete Personendatenbearbeitungen. Für jeden Mandanten einer Direktion oder eines Amts ist deshalb ein ergänzendes ISDS-Konzept zu erstellen und der DSA zur Vorabkontrolle vorzulegen. Dabei wird namentlich geprüft, welche Personendaten bearbeitet werden – wo Ämter mit Fachapplikationen arbeiten, sind es unter Umständen nur die Mitarbeiterdaten – und ob der Zugang zu besonders schutzwürdigen Daten angemessen eingeschränkt wird (dies ergibt sich aus dem Ordnungssystem und den Organisationsvorschriften). Weiter werden die Regelungen zur Aufbewahrung und Archivierung plausibilisiert sowie geprüft, wie die Rechte der betroffenen Personen (insbesondere Auskunft/Einsicht und Sperrung) sichergestellt werden.

Kantonaler Arbeitsplatz (KWP) 4.0

Auch die Vorabkontrolle des KWP war insoweit untypisch, als dieser als Grundlage für eine Vielzahl von Datenbearbeitungen in unterschiedlichsten Applikationen dient. Daher galt als SOLL-Anforderung an das System, dass damit auch besonders schützenswerte Personendaten bearbeitet werden können und dabei genügend gesichert sind. Ob das System diese Anforderungen auch im tatsächlichen Betrieb (IST) erfüllen kann, wurde im Anschluss mittels eines Audits überprüft (siehe unten Ziff. 6 Bst. d).

«Suisse ePolice deux»

Die Applikation «Suisse ePolice deux» ist ein Bürgerportal, über welches kleinere Delikte und Ereignisse mit polizeilichem Bezug an das jeweils zuständige kantonale Polizeikorps gemeldet werden können. Die Applikation wird vom Verein HPi (Harmonisierung der Schweizer Polizeiinformatik), dem alle kantonalen Polizeikorps angehören, betrieben. Die Vorabkontrolle wurde von der KAPO als für ihren

Zuständigkeitsbereich verantwortliche Behörde initiiert, es bestand jedoch der Wunsch, dass die DSA die Prüfung mit Geltung für alle beteiligten Kantone durchführte, was nach der gegenwärtigen Rechtslage formell nicht möglich war. Die eingereichten Dokumente wiesen einen hohen Reifegrad auf, so dass die Vorabkontrolle erfolgreich – wenn auch erst nach Inbetriebnahme der Applikation – abgeschlossen werden konnte. Mit Zustimmung des Vereins HPi stellte die DSA ihren Vorabkontrollbericht anderen kantonalen Aufsichtsstellen zur Kenntnis zu. Der schweizweite Anwendungsbereich der Applikation zeigte einmal mehr den Bedarf nach einer Koordination der kantonalen Datenschutzaufsichtsstellen auf.

Weitere Fachapplikationen der KAPO

Auch rein «innerkantonal» legte die KAPO zahlreiche Systeme und Applikationen – namentlich ein System zur Abfrage verschiedener polizeilicher Informationssysteme, ein Einsatzleitsystem sowie den GEVER-Mandanten der KAPO – zur Vorabkontrolle vor. Dabei bewährte es sich, dass die grundlegenden Sicherheitsanforderungen (z.B. betreffend Standort und Schutz des Rechenzentrums) in einem von der DSA geprüften Grundschutz-Konzept dokumentiert und umgesetzt wurden, so dass jene Aspekte nicht in jeder Vorabkontrolle erneut geprüft werden mussten.

«Competella»

Mit dem Competella Management-Tool können die kantonalen Verwaltungs- und Justizbehörden Telefonie-Randdaten (u.a. wer mit wem wie lange telefoniert; welche Anrufe von wem wie schnell beantwortet oder unbeantwortet abgebrochen werden etc.) umfassend auswerten. Eine solche Auswertung ist sowohl für das Kantonspersonal als auch für die Kunden in hohem Mass datenschutzrelevant. Das Vorabkontrollverfahren war bei der Verfassung des vorliegenden Berichts noch nicht abgeschlossen. Fest steht, dass solche Auswertungen nur in den engen Grenzen der neuen Bestimmungen des Personalgesetzes für die Bearbeitung von Randdaten und der zugehörigen RDV zulässig sind (siehe oben Ziff. 6 Bst. b).

Brust-Screening-Programm «Donna»

Die DSA hatte im Vorjahr bereits das bern-jurassische Brust-Screening-Programm «BEJUNE» vorabkontrolliert. Im Jahr 2019 folgte die Kontrolle des Screening-Programms «Donna», mit dem das übrige Kantonsgebiet nebst dem Berner Jura abgedeckt wird. Hier lag das Augenmerk vor allem auf den Arbeitsabläufen und Datenflüssen: von der Einladung der Frauen der betreffenden Alterskategorie bis zur Eröffnung des Bescheids an diese sowie an den von ihnen beauftragten Arzt. Ebenfalls Gegenstand der Kontrolle war der Datenfluss zum kantonalen Krebsregister. Die Vorabkontrolle konnte erfolgreich und ohne wesentliche Befunde abgeschlossen werden.

Gelegentlich wurde die DSA bereits frühzeitig zur Frage der Vorabkontrollpflicht bzw. zum sinnvollen Vorgehen konsultiert oder führte eine solche zu Schulungszwecken durch, obwohl formell keine Pflicht gegeben war:

«SOCOM»

Der DSA wurde die ISDS-Analyse zur Applikation SOCOM zur Klärung der Frage eingereicht, ob eine Vorabkontrolle nötig sei. SOCOM ist eine Software zur vereinfachten Abwicklung von Anmeldung, Durchführung und Abrechnung von öffentlichen Schlachtviehmärkten. Die summarische Durchsicht ergab, dass mit SOCOM weder besonders schützenswerte Daten noch Daten, die durch eine Geheimhaltungspflicht geschützt sind, bearbeitet werden. Damit war keine Vorabkontrolle nach Art. 17a KDSG nötig. Dieses Ergebnis wurde zusammen mit einigen Hinweisen zu ISDS-Schutzmassnahmen dem zuständigen IT-Sicherheitsverantwortlichen mitgeteilt.

Datenschutzkonzept der Reha-Klinik Schönberg Gunten

Nach dem Motto «Datenschutz ist auch Chefsache» unterbreitete der Direktor der Klinik Schönberg Gunten der DSA das interne Datenschutzkonzept mit der Bitte um Stellungnahme und Beratung. In der anschliessenden interdisziplinären Besprechung (Technik und Recht) wurde das Verfahren zur Erarbeitung eines umfassenden ISDS-Konzepts festgelegt. In einem ersten Schritt wird nun eine Dokumentation der Infrastruktur mit den damit zusammenhängenden Grundschutzmassnahmen gefertigt und der DSA zur Vorabkontrolle vorgelegt (untypische Vorabkontrolle). Danach sollen auf der Grundlage der erstellten Dokumentation applikationsspezifische Unterlagen wie z. B. für das System der Behandlungsdokumentation (Klinikinformationssystem) erstellt werden.

«MELBA»

In der Applikation MELBA des Amtes für Justizvollzug (AJV) werden persönliche und soziale Kompetenzen von Personen im Strafvollzug sowie die Anforderungen an Arbeiten verwaltet, um die Übereinstimmung von Qualifikationen und Einsatzort gut aufeinander abstimmen zu können. Die erfassten Personendaten sind besonders schützenswert, die Anzahl der betroffenen Personen ist aber so gering, dass eine formelle Vorabkontrolle nicht notwendig gewesen wäre. Weil die für MELBA zuständige neue Projektleiterin des AJV künftig auch vorabkontrollpflichtige Vorhaben verantworten wird, wurde die Vorabkontrolle zu Schulungszwecken trotzdem fachgerecht durchgeführt, was sich sehr gelohnt hat: Die gestützt auf die Feststellungen der DSA nachgebesserte Dokumentation war sehr viel besser, so dass die Vorabkontrolle ohne verbleibende Befunde abgeschlossen werden konnte.

6.3.2 Videoüberwachungen

Schule für Gestaltung

Die für die Bewilligung zuständige KAPO unterbreitete der DSA die Unterlagen für eine Videoüberwachung der Schule für Gestaltung des Kantons Bern (SfG) zur Vorabkontrolle. Die Überwachung dient einerseits dem Schutz vor Vandalismus, Sachbeschädigungen, Diebstählen etc. und andererseits dem gezielten Schutz von künstlerischen Exponaten, welche die Schule als Teil der «Museen Bern» in ihren Räumlichkeiten ausstellt. Die Überwachung besteht aus 14 Kameras mit einer generellen Aufzeichnung während 7 Tagen x 24 Stunden. Die DSA liess sich die Überwachung von der SfG vor Ort zeigen. Sie kam zum Schluss, dass an einzelnen Orten (Schulhausrestaurant inkl. Aussenterrassen und Eingangstüren) während der Öffnungszeiten des Restaurants die soziale Kontrolle durch den Publikumsverkehr genügte und eine Aufzeichnung einen unnötigen Eingriff in die Privatsphäre der Schülerinnen und Schüler, des Personals und externer Besucher darstelle. Keine Einschränkungen verlangte sie für die Kameras, die gezielt dem Schutz der Exponate dienen. Insgesamt befand sie, dass die Videoüberwachung noch deutlicher, d.h. gut sichtbar zu kennzeichnen sei.

Spital Aarberg

Das zur Insel Gruppe gehörende Spital Aarberg reichte bei der DSA die Unterlagen zu einer Echtzeit-Videoüberwachung mit sechs Kameras zur Sicherstellung der Notfallversorgung des Spitals ein. Weil diese Videoüberwachung keinen polizeilichen Sicherheitszwecken dient, sondern das Spital bei seiner Aufgabenerfüllung im Dienst der Patientinnen und Patienten unterstützt, war bloss eine datenschutzrechtliche Vorabkontrolle und keine Bewilligung durch die KAPO erforderlich. Die DSA befand, dass die Videoüberwachung datenschutzkonform betrieben werden kann, wenn die nötigen technischen und organisatorischen Massnahmen zum Schutz der Bilder und des übrigen Spitalnetzwerkes – namentlich Betrieb der Kameras in einem eigenen Kameranetzwerk, verschlüsselte Übertragung der Bilder und passwortgeschützte Zugriffe auf jene – getroffen werden.

6.4 Audits

Im Berichtsjahr wurden sechs Prüfungen im Bereich ISDS durchgeführt und bei sieben abgeschlossenen ISDS-Prüfungen aus den Jahren 2016–2018 die laufende Umsetzung der Massnamen begleitet. Bei diesen Folgearbeiten konnte generell ein Fortschritt festgestellt werden, wobei auch klar erkennbar wurde, dass die Umsetzung von teils umfangreichen Massnahmen entsprechend zeit- und ressourcenintensiv ist.

Spital Region Oberaargau SRO AG

Die SRO ist das regionale Spitalzentrum im Oberaargau. Neben dem Spital Langenthal werden Gesundheitszentren und Wohneinrichtungen betrieben. Die SRO verfügt über circa 190 Betten, 8600 stationäre und 49000 ambulante Patienten pro Jahr und beschäftigt circa 1100 Mitarbeitende. Der Betrieb der ICT-Infrastruktur wird grösstenteils mit internen Ressourcen sichergestellt. Im Rahmen von Projekten und für Dienstleistungen werden externe Spezialisten hinzugezogen. Es werden circa 1300 ICT-Arbeitsplätze mit den technischen Basissystemen zentral betrieben und verwaltet. Zum Zeitpunkt der Prüfung befanden sich im ICT-Infrastruktur-Bereich grössere Vorhaben in Arbeit oder in Planung.

Die Prüfung des ICT-Grundschutzes umfasste die Bereiche ISDS-Steuerung und -Lenkung, die ISDS-Konzepte und -Schutzmassnahmen, das Zugriffsmanagement, die Datenverwaltung, die Netzwerk-, Server- und Clientsicherheit, das Veränderungsmanagement, die Vereinbarungen mit Dritten (Outsourcing) sowie die physische Sicherheit vor Ort (Serverräume).

Das Gesamtergebnis der Prüfung weist in allen Prüfbereichen ein deutliches Verbesserungs- und Optimierungspotential aus. Die Prüfung zeigte auf, dass sich der Bereich ISDS in einem organisatorisch komplexen Spitalumfeld mit einem heterogenen Technologie- und Technikumfeld kontinuierlich behaupten muss, insbesondere, weil die vor dem Hintergrund des allgemeinen Kostendrucks bereitgestellten Ressourcen begrenzt sind. Die Prüfung ergab aber auch, dass bereits sehr grosse Anstrengungen unternommen wurden, um bestehende Defizite und damit ISDS-Risiken mit geeigneten Massnahmen zu mindern. Die Prüfung erfolgte in einem sehr professionellen und konstruktiven Umfeld.

Die DSA wird die Umsetzung der Verbesserungsmassnahmen begleiten. Weiter plant die DSA im Bereich der Medizinaltechnik eine Folgeprüfung durchzuführen.

Windows 10-Clients für die Schulen

Die Erziehungsdirektion (heute: Bildungs- und Kulturdirektion) stellt im Rahmen des EDUBERN-Angebots unter anderem Windows 10-Clients (eduClient) für die kantonalen Schulen zur Verfügung.

Die Prüfung umfasste die Bereiche ISDS-Steuerung und -Lenkung sowie entsprechende Kontrollen, die Client-Schutzmassnahmen, die Verwaltung der Windows 10-Clients, das Nutzerverhalten, die bestehenden Benutzerprofile und die Zugriffsrechte, den vorhandenen Malware-Schutz sowie das Veränderungsmanagement.

Das Gesamtergebnis der Prüfung weist über alle Prüfbereiche hinweg ein Verbesserungs- und Optimierungspotential aus. Generell konnte aber festgestellt werden, dass die verwalteten Windows 10-Clients bereits zum grossen Teil den

bestehenden ISDS-Anforderungen entsprechen und weitgehend über die erwarteten technischen Schutzmassnahmen gemäss anerkannten Grundschutz-Standards und Richtlinien verfügen. Defizite bestehen etwa bei der klaren Zuordnung der Verantwortlichkeiten betreffend ISDS bei der Datenbearbeitung auf den zur Verfügung gestellten Windows 10-Clients; insbesondere die Pflichten der Schulen als Leistungsbezüger und Datenbearbeiter müssen eindeutig definiert werden. Weiter wurde festgestellt, dass der «sprunghafte» Einsatz von Technologien – z.B. Cloud-Nutzung, Apps etc. – im Schulumfeld weitergehende Datenschutzfragen aufwirft, welche in Anbetracht der gängigen Praxis der sich rasch verändernden Technik bestmöglich beantwortet werden müssen. Die Zusammenarbeit war professionell und zielführend.

Die DSA wird die Umsetzung der Verbesserungsmassnahmen begleiten.

Drahtloses Netzwerk der kantonalen Verwaltung

Das KAIO stellt im Rahmen der ICT-Grundversorgung den Service BE-Net WLAN (drahtloses Netzwerk) zur Verfügung. Der WLAN-Service bildet die Grundlage für den drahtlosen Zugriff von Clients auf das kantonale Netzwerk. Zum Zeitpunkt der Prüfung wurden circa 1000 aktive Access Points (Zugangspunkte) an über 100 Standorten verwaltet. Das WLAN wird durch einen externen Dienstleister betrieben.

Für die WLAN-Prüfung wurden dezidierte Standorte und WLAN-Netzwerke festgelegt. Dabei wurde darauf geachtet, dass es sich bei den gewählten Standorten um solche mit hohem Publikumsverkehr handelt. Das Risiko von beabsichtigtem oder unbeabsichtigtem Eindringen in das kantonale Netzwerk kann an solchen Standorten erhöht sein. Die Prüfung umfasste primär die Beurteilung der WLAN-Sicherheit und -Robustheit. Betriebliche Prozesse wie die systematische Änderungskontrolle (Change- und Release-Management), das Konfigurations-Management, das Monitoring, die physische Sicherheit vor Ort, die Netzwerkabsicherung und die bestehende Netzwerkzonierung wurden ebenfalls geprüft. Das Gesamtergebnis der Prüfung weist über alle Prüfbereiche hinweg ein punktuelles Verbesserungs- und Optimierungspotential aus. Zusammenfassend konnte aber festgestellt werden, dass der operative WLAN-Betrieb grösstenteils den bestehenden Sicherheitsanforderungen entspricht und die verwendete technische Infrastruktur über weitgehend adäquate technische Schutzmassnahmen verfügt. Defizite bestehen insbesondere im Bereich des systematischen und kontinuierlichen Monitorings und bei der zeitnahen Reaktion im Fall von Störungen und Anomalien. Die Prüfung erfolgte in einem professionellen Umfeld.

Die empfohlenen Verbesserungsmassnahmen sind bereits teilweise umgesetzt worden oder befinden sich noch in Arbeit. Die DSA wird über den Verlauf der Umsetzung der Verbesserungsmassnahmen informiert.

Kantonaler Arbeitsplatz (KWP)

Der KWP bildet in der ICT-Grundversorgung des Kantons Bern die technische Grundlage für die Nutzung der Fach- und Konzernapplikationen. Die Vorabkontrolle der DSA hatte ergeben, dass der SOLL-Beschrieb des KWP 4.0-Client, welcher durch das KAIO bzw. einen externen Dienstleister bereitgestellt wird, die bestehenden ISDS-Anforderungen noch nicht vollständig erfüllt (siehe oben Ziff. 6 Bst. c).

Die in der Folge angesetzte Prüfung des KWP 4.0 (IST) umfasste Interviews mit den verantwortlichen Personen, Reviews von relevanten Dokumenten und die Durchführung von technischen Sicherheitstests zur Erkennung und Offenlegung von möglichen konzeptionellen und technischen Sicherheitslücken im ISDS-Bereich.

Das Gesamtergebnis der Prüfung zeigte auf, dass aus konzeptioneller Sicht die involvierten verantwortlichen Parteien bereits gut aufgestellt sind. Viele organisatorische Massnahmen, welche den sicheren Betrieb des KWP 4.0 gewährleisten, sind bereits umgesetzt oder befinden sich in der Planung. Aus technischer Sicht ist der KWP 4.0 fachkompetent konfiguriert und bezeugt umfassendes technisches Know-how der Verantwortlichen. Trotzdem wurden in allen Prüfgebieten Schwachstellen erkannt, welche noch verbessert werden sollten. Die Zusammenarbeit mit allen beteiligten Stellen war professionell und vorbildlich.

Die DSA wird über den Verlauf der Umsetzung von Verbesserungsmassnahmen informiert.

Klinik Südhang

Die Klinik Südhang ist ein Kompetenzzentrum für Mensch und Sucht und bietet Menschen mit einer Suchterkrankung spezialisierte Unterstützung. Zu den Regionalen Ambulanten Diensten Südhang gehören die Tagesklinik Bern, das Ambulatorium Bern sowie die Ambulatorien in Burgdorf und Biel-Bienne.
Im 2018 erfolgte eine massgebende Veränderung der ICT-Infrastruktur. Die Klinik Südhang verwaltet und betreibt ihre technische Client- und Server-Infrastruktur sowie die Fachanwendungen mit externer Unterstützung.

Die Prüfung umfasste primär die ISDS-Steuerung und -Lenkung sowie die Umsetzung des ISDS-Konzepts mit den notwendigen Schutzmassnahmen und die Vereinbarungen mit externen Leistungserbringern.

Das Gesamtergebnis der Prüfung weist über alle Prüfbereiche hinweg ein Verbesserungs- und Optimierungspotential aus. Zusammenfassend konnte festgehalten werden, dass die zahlreichen ISDS-Aufgaben, die sich im Rahmen der betrieblichen (Sicherheits- und Betriebsprozesse, Kontrollen etc.), aber auch der strategischen ISDS-Steuerung ergeben, eine grosse Herausforderung

für die bestehende Organisation darstellt. Die Klinik Südhang wird deshalb zusätzliche Ressourcen bereitstellen und die bestehenden ISDS-Risiken und -Defizite mit entsprechenden Massnahmen kontinuierlich mindern. Die Zusammenarbeit erfolgte in einem professionellen und kooperativen Umfeld.

Die DSA wird die Umsetzung der Verbesserungsmassnahmen begleiten.

Schengener Informationssystem (SIS)

Mit der Übernahme des Schengen-Acquis verpflichtete sich die Schweiz, die datenschutzkonforme Nutzung des SIS zu gewährleisten und periodisch zu prüfen. Letzteres ist im Kanton Bern die Aufgabe der DSA. Diese prüfte im Herbst 2019 die Zugriffe durch die Regionalpolizei Seeland-Berner Jura. Bei den von ihr überprüften Abrufen stellte sie fest, dass das SIS für polizeiliche Aufgaben konform genutzt wurde. So lagen keine offensichtlichen Unregelmässigkeiten wie z.B. Abfragen zur eigenen Person oder von Personen des öffentlichen Lebens vor. Allerdings stellte sie einen Mangel an regelmässiger Schulung und Information zum SIS fest. Sie empfahl deshalb, diesen Mangel zu beheben. Die KAPO nahm die Empfehlung an und definierte neue Informations- und Schulungsmassnahmen.

6.5 Weitere aufsichtsrechtliche Instrumente

Liquidation Verwaltungsbeschwerde zu BE-GEVER

Eine bei der Finanzdirektion hängige Beschwerde der DSA gegen das KAIO betreffend die Einführung von BE-GEVER in einer Direktion wurde durch Vergleich beigelegt. Darin verpflichtet sich das KAIO, sich bestmöglich für die Einführung einer Zwei-Faktoren-Authentisierung (2FA) auf dem KWP ab 2020 einzusetzen. Der Einsatz zusätzlicher Authentisierungsmerkmale (nebst einem Passwort als Wissenselement) bei der Anmeldung am Arbeitsplatz erhöht die Sicherheit, dass die angemeldete Person tatsächlich jene ist, die vom System erkannt und zugelassen wird, und gilt heute als Standard für die Bearbeitung von besonders schützenswerten Personendaten. Eine starke Authentisierung am KWP erlaubt es, dass auf diesem laufende Konzern- und Fachapplikationen auf eine eigene 2FA verzichten können. Im Vergleich anerkennt die DSA, dass der Einsatz einer digitalen Signatur keine datenschutzrechtliche Anforderung an ein GEVER-System darstellt. Auf die ebenfalls offene Frage der Datenschutzverantwortung in einer arbeitsteiligen Verwaltungsorganisation – das KAIO verantwortet die Grundversorgung und gewisse Applikationen, die Direktionen und Ämter

verantworten den Einsatz der Fachapplikationen in ihrem Zuständigkeitsbereich – wurde im Hinblick auf ein neues Gesetz über die digitale Verwaltung ein Lösungsvorschlag formuliert.

Im Jahr 2019 wurden kein begründeter Antrag nach Art. 35 Abs. 3 KDSG gestellt und keine Verwaltungs- oder Verwaltungsgerichtsbeschwerde erhoben.

Oberaufsicht über die Aufsichtsstellen der Gemeinden

Als Ausfluss der Gemeindeautonomie sieht das KDSG vor, dass jede Gemeinde für ihren Bereich eine eigene Aufsichtsstelle bezeichnet; die DSA übt die Oberaufsicht aus. Gegenwärtig nimmt die DSA diese Aufgabe nur passiv – auf Anfrage von kommunalen Aufsichtsstellen oder von betroffenen Personen – wahr. Dabei stellt sie teils erhebliche Unterschiede in der Verfügbarkeit und Qualität der kommunalen Datenschutzaufsicht fest. Anspruchsvolle Rechtsfragen und technische Problemstellungen bringen die Gemeindebehörden und ihre Aufsichtsstellen oftmals an fachliche Grenzen, und diese fragen sich, warum sie Themen, welche jede der über 300 bernischen Gemeinden gleichermassen beschäftigen dürften (z.B. bei der Digitalisierung der Volksschule, siehe oben Ziff. 6 Bst. a), überhaupt auf kommunaler Ebene bearbeiten müssen. Im Hinblick auf die Revision des KDSG erarbeitet die DSA Vorschläge, wie die Unterstützung der Gemeindebehörden in ISDS-Fragen verbessert werden könnte.

7 Antrag

Kenntnisnahme.

8 Glossar / Abkürzungen

DSA	Datenschutzaufsichtsstelle des Kantons Bern
DSG	Datenschutzgesetz des Bundes
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EV EDS	Einführungsverordnung zur EU-Datenschutzrichtlinie
EV KRG	Einführungsverordnung zur eidgenössischen Krebsregistrierungsgesetzgebung
FK	Finanzkontrolle
GERES	Gemeinderegistersystem
GEVER	(Elektronische) Geschäftsverwaltung
GEF	Gesundheits- und Fürsorgedirektion (heute: GSI)
GSI	Gesundheits-, Sozial- und Integrationsdirektion
HPi	Harmonisierung der Schweizer Polizeiinformatik
ICT	Informations- und Telekommunikationstechnik
IP	Internet Protocol
ISDS	Informationssicherheit und Datenschutz
IT	Informatik
KAIO	Kantonales Amt für Informatik und Organisation
KAPO	Kantonspolizei
KDSG	Kantonales Datenschutzgesetz
KESB	Kindes- und Erwachsenenschutzbehörde
KWP	Kantonaler Arbeitsplatz
LKG	Landeskirchengesetz
PDSG	Personendatensammlungsgesetz
POM	Polizei- und Militärdirektion (heute: Sicherheitsdirektion)
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
RDV	Randdatenverordnung
SfG	Schule für Gestaltung
SIS	Schengener Informationssystem
SpVG	Spitalversorgungsgesetz

SRO	Spital Region Oberaargau
TCHF	Tausend Franken
WLAN	Drahtloses Netzwerk
ZPV	Zentrale Personenverwaltung
2FA	Zwei-Faktoren-Authentisierung

Datenschutzaufsichtsstelle
des Kantons Bern

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

www.be.ch/dsa