Bericht 2018 der Datenschutzaufsichtsstelle des Kantons Bern

Datenschutzaufsichtsstelle des Kantons Bern
Poststrasse 25
3072 Ostermundigen
Telefon 031 633 74 10
Telefax 031 634 51 53
datenschutz@be.ch
www.be.ch/dsa

Inhalt

1 Einleitung

1.1 Auf einen Blick

Am 8. Januar 2019 verabschiedete der Regierungsrat unter dem Begriff «Engagement 2030» seine Regierungsrichtlinien 2019–2022. Ein Ziel lautet dahingehend, dass der Kanton Bern die Chance der digitalen Transformation nutzen und wirkungsvolle, qualitativ hochstehende und effiziente Dienstleistungen für Bevölkerung und Wirtschaft erbringen soll. Am 5. März 2019 veröffentlichten die Geschäftsstelle E-Government Schweiz und das Staatssekretariat für Wirtschaft mit der Nationalen E-Government-Studie 2019 die zweite Ausgabe einer repräsentativen Erhebung bei Bevölkerung, Unternehmen und Verwaltungen der Schweiz zum Thema. Danach haben 68% der Bevölkerung Vertrauen in die Online-Dienstleistungen der kantonalen Behörden bezüglich Persönlichkeits- und Datenschutz. Der Wert entspricht in etwa jenem der ersten Studie vom November 2017, wo auch die kantonalen Behörden nach ihrer Einschätzung des Vertrauens der Bevölkerung in ihre Online-Dienste befragt wurden und jenes auf 95% bezifferten. Eine Befragung zum Vertrauen in die behördeninternen elektronischen Datenbearbeitungen dürfte ähnliche Ergebnisse – und eine ebenso grosse Differenz zwischen den Einschätzungen der Bürger und der Verwaltung – hervorbringen. Es ist deshalb zentral, dass die Behörden Datenschutz und -sicherheit nicht nur als rechtliche Rahmenbedingung – und insoweit als «Bremser» – der digitalen Transformation verstehen, sondern ebenso als Erfolgsfaktor für die Akzeptanz und den Erfolg eines weiteren Ausbaus von E-Government.

Vor diesem Hintergrund sind die mannigfaltigen Arbeiten der Datenschutzaufsichtsstelle im Jahr 2018 – die Kontrolle von in Betrieb stehenden Informatikanwendungen (unten Ziff. 3), die Vorabkontrolle von Videoüberwachungsanlagen (Ziff. 4) und einer Vielzahl von Informatikprojekten (Ziff. 5), die Stellungnahme zu datenschutzrechtlichen Anfragen von kantonalen Behörden und Gemeinden (Ziff. 6) einschliesslich der Mitwirkung bei der Vorbereitung von Erlassen (Ziff. 7) sowie selbst die Eskalation von Differenzen in verwaltungsinternen und -gerichtlichen Beschwerdeverfahren (Ziff. 8) – nicht nur als vom Gesetzgeber vorgesehene Kontrolle der Verwaltung zu sehen, sondern auch als Dienstleistung zu deren Gunsten.

1.2 Zusammenarbeit mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sowie der Konferenz der Schweizerischen Datenschutzbeauftragten (privatim)

Die Datenschutzaufsichtsstelle (DSA) nahm im Berichtsjahr an einer Sitzung der Koordinationsgruppe des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) teil, mittels derer der EDÖB die Aufsicht über das Schengener Informationssystem (SIS) koordiniert. 2018 erhielt die Aufsichtsstelle die nötigen Logfiles vom Bundesamt für Polizei (fedpol) nicht fristgerecht, so dass die geplante Kontrolle der SIS-Abfragen bei der Kantonspolizei Bern nicht stattfinden konnte. Da Aufsichtsstellen anderer Kantone teilweise ähnliche Erfahrungen gemacht hatten, beschloss die Koordinationsgruppe des EDÖB bei fedpol ein klares, einheitliches Prozedere für den Erhalt der Logfiles zu verlangen.

Sodann wirkte die DSA in mehreren privatim-Arbeitsgruppen (AG) und an einem Workshop zum Thema Anforderungen an Cloudlösungen mit. Die AG «Digitale Verwaltung» beschäftigte sich in mehreren Sitzungen mit verschiedenen Themen einer digitalen Verwaltung: so mit Anforderungen an Online-Portale, den Bundesprojekten e-ID und e-Voting. Im Berichtsjahr entstand ein Merkblatt für Online-Portale der Verwaltung, welches am folgenden Ort publiziert ist: http://www.privatim.ch/de/publikationen/.

Die AG Gesundheit befasste sich wie im Vorjahr weiterhin mit Fragen des Datenschutzes und der Sicherheit des elektronischen Patientendossiers. Im Frühjahr fand eine Sitzung mit dem Bundesamt für Gesundheit und dem EDÖB zur datenschutzrechtlichen Zuständigkeit statt. Bis zum Berichtszeitpunkt konnten die schwierigen Abgrenzungsfragen noch nicht abschliessend geklärt werden. Aus Ressourcengründen wurde die Mitarbeit der DSA in der AG Gesundheit im März 2018 bis auf weiteres sistiert.

1.3 Änderungen im übergeordneten Recht

Gemäss den Verpflichtungen der Schweiz aus dem Schengen-Assoziierungsabkommen war die von der EU im April 2016 verabschiedete Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr bis am 1. August 2018 im Landesrecht umzusetzen. Mit dem Erlass einer auf vier Jahre befristeten Dringlichkeitsverordnung (Einführungsverordnung vom 04.07.2018 zur EU-Datenschutzrichtlinie) erfüllte der Kanton Bern die

Verpflichtung als zweiter Kanton – nur der Aargau hatte sein kantonales Datenschutzgesetz rechtzeitig revidiert – und vor dem Bund, dessen Schengen-Datenschutzgesetz per 1. März 2019 in Kraft trat. Jetzt wird es darum gehen, die Dringlichkeitsverordnung im Rahmen einer Revision des kantonalen Datenschutzgesetzes in ordentliches Recht zu überführen und dabei das Datenschutzrecht generell auf einen aktuellen Stand zu bringen.

2 Aufgabenumschreibung, Prioritäten und Mittel

2.1 Prioritäten

Gestützt auf Art. 34 Datenschutzgesetz (KDSG) hat die DSA namentlich folgende Aufgaben: Überwachung der Anwendung der Vorschriften über den Datenschutz und der Datensicherung, Vorabkontrolle von Informatikprojekten, Beratung der Verwaltung (Erlasse und Vollzug) und von betroffenen Personen sowie – bei Bedarf – Vermittlung zwischen Behörden und Privaten. Die Aufgaben gemäss KDSG sind grundsätzlich flächendeckend zur erfüllen, wobei bei den gegebenen personellen und finanziellen Ressourcen eine Priorisierung unumgänglich ist. Im Jahr 2018 hat die DSA diese anhand folgender Kriterien vorgenommen:

– Vorschalten der zuständigen Stelle: Die Beratung kommunaler und kantonaler Verwaltungsstellen hat durch die zuständigen kommunalen Datenschutzaufsichtsstellen bzw. Rechtsdienste der kantonalen Verwaltung zu erfolgen. Betroffene sind in kommunalen Fragen durch die kommunalen Datenschutzaufsichtsstellen zu beraten. Wer unmittelbar bei der DSA anfragt, ist an die zuständigen Stellen zu verweisen. Diese Zuständigkeiten und die dadurch notwendige Triage sind in der Datenschutzverordnung verankert.

– Unterschiedliche Qualitätsstandards: Einer betroffenen Person oder einer Milizbehörde wird als Antwort eine Handlungsanweisung ohne nähere rechtliche Begründung genügen. Für eine Stellungnahme an eine Justizinstanz ist dagegen eine umfassende rechtliche Vertiefung erforderlich. Der Qualitätsstandard ist vor Beginn der Arbeit festzulegen.

– Subsidiarität des aufsichtsrechtlichen Handelns: Die Datenschutzgesetzgebung gewährt den Betroffenen gute Abwehrrechte (Berichtigung, Vernichtung, Feststellen der Widerrechtlichkeit). Aufsichtsrechtliche Abklärungen sollen unterbleiben, wenn solche Abwehrmöglichkeiten gegeben sind. Die Betroffenen sind auf ihre Abwehrrechte aufmerksam zu machen. Lassen die Hinweise Rückschlüsse auf Systemprobleme zu, ist diesen mit den entsprechenden Mitteln (z. B. Kontrollen) nachzugehen.

– Vorabkontrollen: Die dafür bestehenden Vorgaben sollen die Projektleitungen zum Umsetzen des Datenschutzes im Projekt veranlassen. Diese Wirkung kann auch erzielt werden, wenn die DSA nur formell das Einreichen der Unterlagen prüft, auf eine inhaltliche Prüfung aber ganz oder zum Teil verzichtet. Ein gesamthafter Verzicht kann dann erfolgen, wenn die gleiche Projektleitung wiederholt korrekte Unterlagen eingereicht hat, ein Projekt untergeordnete Bedeutung hat oder wenn die Gesamtbelastung der DSA eine rechtzeitige Prüfung nicht erlaubt. Teilkontrollen sind insbesondere dann angezeigt, wenn über einzelne Bereiche Aussagen aus früheren Prüfungen möglich sind (z.B. zur Sicherheit der eingesetzten Informatikinfrastruktur) oder wenn Bereiche mit hohen Risiken bekannt sind (z.B. Zugriffsrechte auf besonders schützenswerte Personendaten).

– Verzicht auf eigene Stellungnahmen zu Bundeserlassen: Im Gesetzgebungsverfahren stellen sich aus Sicht aller Kantone regelmässig die gleichen Fragen. Die DSA beschränkt sich darauf, die Stellungnahme von privatim weiterzugeben und allenfalls an dieser mitzuwirken.

Die Zuweisung der Aktivitäten auf die Mitarbeitenden erfolgte nach den Kriterien Region (Gemeinden), kantonale Organisationseinheit (Direktionen) und Fachgebiet (z.B. Staatskirchenrecht). Die Mitarbeitenden setzten die Prioritäten nach den aufgezeigten Kriterien selbständig. Die Priorisierung von Vorabkontrollgeschäften erfolgte nach Eingang gemeinsam mit der Leitung der DSA. War es nicht mehr möglich, die vorgegebenen Antwortzeiten einzuhalten (Leistungsziele), nahmen die Mitarbeitenden eine Änderung der Priorisierung, allenfalls die Zuweisung an andere Mitarbeitende, den (Teil-) Verzicht auf eine Behandlung oder das Senken des Qualitätsstandards nach Rücksprache mit der Leitung der DSA vor. Diese stellte dabei sicher, dass jedenfalls Kontrollen von Informatikanwendungen und Nachbetreuungen dieser Kontrollen stattfinden, und dass trotz Verzichts auf Vorabkontrollen die «Selbststeuerung» durch die Projektleitungen erhalten blieb. Bei Beratungen und aufsichtsrechtlichen Interventionen liegen die Schwerpunkte meist auf den technischen Entwicklungen, die für die Persönlichkeitsrechte der Betroffenen besondere Folgen haben.

2.2 Personelle und finanzielle Mittel

Im Jahr 2018 verfügte die DSA über 5.15 Vollzeitstellen (inkl. Sekretariatsleistungen), und der Betriebsaufwand betrug 149 TCHF. Davon ent-

fielen 119 TCHF auf die Prüfung von Informatikanwendungen durch externe Stellen.

Im Oktober 2018 zog die DSA aus der Innenstadt Bern nach Ostermundigen. Dies und die gleichzeitige Umstellung auf eine neue Geschäftsverwaltungssoftware waren Auslöser für eine umfassende Archivierung der Papierunterlagen der DSA. Weil das Staatsarchiv des Kantons Bern fast alle vorliegenden Papierakten als archivwürdig einstufte, lieferte die DSA Papierakten aus den Jahren 1991–2014 im Umfang von 21.60 Laufmetern (in 216 Archivschachteln) zur Archivierung und Vorarchivierung ab. Im August hatte die DSA ihre Aktenführung vom Papierprimat auf das elektronische Primat umgestellt. Im neuen GEVER-System ist je nach Ordnungsposition neu festgelegt, ob es sich um archivwürdige Geschäfte handelt oder nicht, was künftig einen stark reduzierten Aufwand für die (elektronische) Ablieferung bringen sollte.

3 Kontrollen von Informatikanwendungen, die im Betrieb stehen

Im Berichtsjahr wurden folgende vier Prüfungen durchgeführt:

– Cloudanwendungen Microsoft 365 in der Erziehungsdirektion

Die Informatikdienste der Erziehungsdirektion (ERZ) stellen den Schulen für den Unterrichtsbetrieb auf Wunsch eine Cloud-Infrastruktur zur Verfügung. In einem speziell für diese Bedürfnisse ausgearbeiteten Vertrag mit Microsoft Schweiz sind die rechtlichen Rahmenbedingungen vereinbart worden.

Die Prüfung zeigte eine klare Abgrenzung der Verantwortlichkeiten zwischen Betrieb und Nutzung auf. So sind die ERZ zusammen mit Microsoft verantwortlich für die Bereitstellung der Infrastruktur und Dienste inkl. der Benutzerverwaltung. Die Schulen ihrerseits tragen die Verantwortung für die Dateninhalte, die durch die Nutzung der Applikationen und Systeme generiert werden. Hier fehlte bisher eine klare Regelung und Zuweisung im Rahmen eines Benutzungsreglements.

Die Prüfung zeigte weiter, dass die konforme Bearbeitung besonders schützenswerter Daten in diesen Clouddiensten nur mit grosser Disziplin der Benutzenden gewährleistet werden kann.

Die Verantwortlichen der Erziehungsdirektion zeigten sich sehr kooperativ im Umgang mit den gemachten Feststellungen und ergriffen die notwendigen Massnahmen, um die aufgedeckten Mängel raschmöglich zu beheben.

– Grundschutz bei der PZM Psychiatriezentrum Münsingen AG

Die DSA kontrollierte zusammen mit einer externen Prüfstelle die IT-Grundinfrastruktur der PZM. Es stellte sich heraus, dass die Verantwortlichen für den operativen IT-Betrieb grosse Anstrengungen unternehmen, um die datenschutzkonforme Bearbeitung der sehr heiklen Daten ihrer Institution so gut wie möglich zu gewährleisten.

Im Verlauf der Prüfung zeigten sich trotzdem erhebliche Mängel im Bereich des Datenschutzes wie auch der Informationssicherheit. Diese waren mehrheitlich auf fehlende strategische und taktische Vorgaben zurückzuführen. So fehlen normativen Vorgaben z.B. in Anlehnung an einen anerkannten Standard wie ISO 27001 / 27002 als Grundlage für die Definition und Umsetzung von Massnahmen sowie für die Überprüfung derer Wirksamkeit. Überarbeitungsbedarf zeigte sich auch bei der Zuteilung / Abgrenzung der Verantwortlichkeiten in verschiedenen Bereichen wie Berechtigungen, Applikationen oder Datensammlungen.

In Zusammenarbeit mit der DSA werden die aufgezeigten Feststellungen analysiert und ein Massnahmenplan ausgearbeitet und umgesetzt.

– Grundschutz-Prüfung der IT-Infrastruktur der Kantonspolizei (KAPO)

Die komplexe IT-Infrastruktur der KAPO Bern wurde anfangs 2018 bezüglich den umgesetzten Grundschutzvorgaben geprüft. Die Prüfung sollte den Status der ISDS-Konformität für den IT-Betrieb zeigen und somit den Aufwand für künftige Vorabkontrollen verkleinern. Die erste Prüfung gab Anlass zu gewichtigen Beanstandungen. In enger Zusammenarbeit mit den Verantwortlichen wurden die im Bericht der externen Prüfstelle dokumentierten Feststellungen angegangen, die erforderlichen Massnahmen zeitnah geplant und teilweise bereits umgesetzt. So konnte im Dezember 2018 eine Nachkontrolle durchgeführt werden.

– Informationssicherheit bei Datenbearbeitung mit Mobilgeräten beim Universitätsspital Bern

Die Prüfung der Infrastruktur gestaltete sich schwierig. Zum einen standen die im Auditprogramm vorgängig bezeichneten Auskunftspersonen (inkl. Outsourcingpartner) nicht zur Verfügung, zum anderen wurden bei den Interviews immer wieder grobe Mängel festgestellt, die mit der IT-Grundinfrastruktur oder mit elementaren Prozessen in Zusammenhang stehen. Diese Mängel beeinflussen direkt oder indirekt die geprüfte Datenbearbeitung und können nicht ausgegrenzt werden. Diese Feststellungen stiessen bei der geprüften Stelle auf wenig Akzeptanz.

Der Auditbericht wurde der Geschäftsleitung im Dezember 2018 übermittelt. Die DSA erwartet eine kooperative Haltung, damit die für einen datenschutzkonformen Betrieb dringend notwendigen Massnahmen zeitnah definiert, geplant und umgesetzt werden. Die im Bericht dokumentierten Feststellungen legen eine umfassende Prüfung der Basisinfrastrukturen und der IT-Prozesse nahe.

4 Videoüberwachung

Im Berichtsjahr prüfte die DSA mehrere Videoüberwachungsanlagen für kantonale Gebäude im Vorabkontrollverfahren. Darunter befanden sich u.a. Anlagen der Insel Gruppe AG (Inselspital Frauenklinik/Baubereich 6.1; Inselspital Schlaganfallstation Stroke Unit; Spital Riggisberg). Weiter beurteilte die DSA vorfrageweise geplante Projekte und deren Zulässigkeit im Rahmen der geltenden Rechtsgrundlagen (Aufnahmen von Beratungsgesprächen in der Regionalen Arbeitsvermittlung [RAV] von beco Berner Wirtschaft; Überwachung des Rechtsmedizinisches Instituts RMI und des Areals Engehalde der Universität Bern). Sie erarbeitete Mustervorlagen mit Prüfpunkten für die Vorabkontrolle von Videoüberwachungen, die nicht gestützt auf das Polizeigesetz, sondern eine spezialgesetzlich geregelte Aufgabenerfüllung durchgeführt werden, sowie für Vorabkontrollen durch kommunale Aufsichtsstellen.

Nicht alle Vorhaben waren im geplanten Umfang zulässig: Aufzeichnungen sind schwere Eingriffe in das Grundrecht auf Datenschutz und benötigen eine klare formell-gesetzliche Grundlage. Fehlt eine solche, sind im Rahmen der gesetzlichen Aufgabenerfüllung ausschliesslich Echtzeitüberwachungen zulässig. Aufzeichnungen in den Spitälern und beim RMI, die sich weder auf das Polizeigesetz (kein polizeilicher Zweck, keine öffentlichen und allgemein zugänglichen Gebäude bzw. Räumlichkeiten) noch auf ein anderes Gesetz abstützen können (keine Regelung z.B. im Spitalversorgungsgesetz oder im Universitätsgesetz), sind deshalb nicht zulässig. Auch Aufzeichnungen von Mitarbeiter-Kundengesprächen zur Verbesserungen der Gespräche im RAV dürfen ohne Rechtsgrundlage nicht durchgeführt werden.

Die DSA weist Spitäler regelmässig darauf hin, dass vor einer Herausgabe von Aufzeichnungen mit Bildern von Patientinnen und Patienten an die Kantonspolizei das Kantonsarztamt um Entbindung von den Geheimhaltungspflichten zu ersuchen ist.

Die DSA kam zum Schluss, dass die Überwachung und anschliessende Auswertung von Rauchemissionen mit Hilfe von Kameras durch den Immissionsschutz beco eine ausdrückliche Grundlage in der kantonalen Lufthygieneverordnung benötigt.

5 Vorabkontrollen von Informatikprojekten

Die DSA prüfte erneut eine hohe Anzahl von Informatikprojekten. Im Folgenden werden in nicht abschliessender Aufzählung Beispiele laufender und erledigter Vorabkontrollen des Berichtsjahres aufgeführt.

5.1 Laufende Vorabkontrollen

– BE-GEVER

Im Hinblick auf die kantonsweite Einführung einer neuen elektronischen Geschäftsverwaltung (BE-GEVER) hatte die DSA bereits im Vorjahr von verschiedenen Amtsstellen ISDS-Konzepte für ihre jeweiligen Mandanten zur Vorabkontrolle eingefordert bzw. erhalten. Sie hatte verlangt, dass der Zugang zu den Systemen mit einer Zwei-Faktor-Authentifikation abgesichert werde und Dokumente digital signiert abzulegen seien. Gegenüber vier Amtsstellen der Finanzdirektion (FIN) hatte sie begründete Empfehlungen ausgesprochen, deren Behandlung die FIN an sich gezogen und bis zum Urteil des Verwaltungsgerichts in der Beschwerdesache 100.2017.72U (siehe unten Ziff. 8) sistiert hatte. Gegen diese Verfügungen erhobene Verwaltungsgerichtsbeschwerden zog die DSA im März 2018 zurück und sprach stattdessen eine Aufforderung aus, die Massnahmen zur Beseitigung der Mängel in BE-GEVER seien unverzüglich zu ergreifen.

In zwei Fällen (BE-GEVER generell und mobiles Sitzungsmanagement in der Gesundheits- und Fürsorgedirektion) erhob die DSA im November 2018 Verwaltungsbeschwerde an die FIN, weil unter Verweis auf die neue Verordnung über die Informations- und Telekommunikationstechnik der Kantonsverwaltung (ICTV) anstelle der GEF als Adressatin der begründeten Empfehlungen das KAIO ablehnende Verfügungen gemäss Art. 35 Abs. 4 KDSG erlassen hatte.

– Competella Management Tool

Eine Anfrage wies die DSA auf das Competella Management Tool hin, das von den kantonalen Verwaltungs- und Justizbehörden als Teil der ICT-Grundversorgung vom Amt für Informatik und Organisation (KAIO) bezogen werden kann. Das Tool ermöglicht eine umfassende Auswertung der anfallenden Telefonie-Randdaten (u.a. wer mit wem wie lange telefoniert; welche Anrufe von wem wie schnell beantwortet oder unbeantwortet abgebrochen werden etc.). Da eine solche Auswertung sowohl für das Kantonspersonal als auch für die Kunden in hohem Mass datenschutzrelevant ist, reichte die DSA eine aufsichtsrechtliche Rückfrage beim zuständigen

Amt ein, um Aufschluss über den Einsatz des Tools und eine Vorabkontrolle zu erhalten. In der Folge informierte das KAIO die Bezüger des Tools über die Notwendigkeit der Vorabkontrolle und empfahl, bis dahin auf die Nutzung der Auswertungsfunktionen ohne ausreichende (eigene) Rechtsgrundlagen zu verzichten.

– Electronic Monitoring EM

Die Applikation Electronic Monitoring (EM) des Amtes für Justizvollzug erlaubt es, gestützt auf Bundesrecht freiheitsentziehende strafrechtliche Sanktionen für Erwachsene und Jugendliche sowie ambulante Massnahmen (wie z.B. Hausarrest) elektronisch zu überwachen. Sämtliche Daten sind besonders schützenswert. Der Kanton Bern schloss sich der per 1. Januar 2018 der EM-Technik-Lösung des Kantons Zürich an. Spätestens per 1. Januar 2023 soll eine nationale Lösung in Betrieb genommen werden. Für die Bearbeitung, Aufbewahrung und Vernichtung der Daten wurden mit dem Justizvollzugsgesetz und den Ausführungserlassen die kantonalen Rechtsgrundlagen geschaffen (siehe unten Ziff. 7.2). Die Vorabkontrolle der überarbeiteten Unterlagen ist noch nicht abgeschlossen.

– ERP

Das KAIO zog die DSA bereits im Rahmen der Konzeptphase für erste Hinweise zu einem kantonalen Enterprise-Resource-Planning (ERP) System für die Supportbereiche Finanzen, Personal und Logistik bei. Im Zentrum standen die Anforderungen an eine Cloud-Lösung.

– Fabesys (Gina-Web)

Mit Fabesys wird das Fallbearbeitungssystem Gina-Web im Amt für Justizvollzug (AJV) eingeführt. Damit wird das heutige System durch eine webbasierte, ablauforientierte Lösung ersetzt. Die Vorabkontrolle konnte in mehreren Schritten durchgeführt werden und stand Ende Berichtsjahr vor dem Abschluss.

– GERES

Die Vorabkontrolle zum kantonalen Personenregister GERES des KAIO ergab u.a., dass für den Zugriff via Internet und Citrix eine Zwei-Faktoren-Authentisierung zu realisieren ist. Zu ergänzen sind Nachweise zur datenschutzkonformen Aufbewahrung der Daten und Logs, der nach wie vor fehlende VIP-Schutz der Daten (Art. 14 KDSG) sowie die technischen Massnahmen, die vor einem missbräuchlichen Datenabruf schützen.

– NewParePas

Die Vorabkontrolle einer Applikation der Justiz-, Gemeinde- und Kirchendirektion zur Bewirtschaftung der Kirchgemeinden und Pfarrstellen stand am Ende des Berichtsjahrs kurz vor dem Abschluss.

5.2 Abgeschlossene Vorabkontrollen

Folgende Vorabkontrollverfahren konnten abgeschlossen werden:

– CoreService WLAN

Die zugehörigen ISDS-Unterlagen wurden nach einer Überarbeitung durch das KAIO von einer externen Firma auditiert. Gestützt auf deren Bericht erledigte das KAIO die offenen Punkte, so dass die Vorabkontrolle abgeschlossen werden konnte. Aus Sicht der DSA wird mit dem neuen SSD-Standard «BEdirect» die Sicherheit gegenüber dem früheren SSD-Standard «BEintern» herabgesetzt, weshalb der CoreService für ein Audit im Jahr 2019 vorgemerkt wurde.

– CRM BFH

Mit dem neuen Customer Relationship Management (CRM) der Berner Fachhochschule (BFH) sollen ein Adressmanagement und ein Kampagnenmanagement eingeführt werden. Die Zugriffsberechtigungen sind sehr weit ausgestaltet und die Mengengerüste sind gross. Da jedoch keine besonders schützenswerten Personendaten bearbeitet werden, ist dies für die DSA gerade noch hinnehmbar. Die letzten Anpassungen in den ISDS-Unterlagen sind durch die BFH in Eigenverantwortung noch vorzunehmen.

– eBau

Die Vorabkontrolle zu einer elektronischen Abwicklung des Baubewilligungsverfahrens wurde abgeschlossen unter der Voraussetzung, dass noch einige Auflagen (Zugriff von Gemeinden und Fachbehörden über BE-Login, Sicherstellen der technischen und organisatorischen Massnahmen für eine datenschutzkonforme Bearbeitung durch die Geräte und Korrekturen bei der Berechtigungsmatrix) umgesetzt werden.

– Elektronisches Personaldossier

Die technische Vorabkontrolle des eDossiers erforderte mehrere Durchläufe, bis die verlangte Informationssicherheit ausgewiesen war. Die juristische Prüfung bestätigte eine verhältnismässige Ausgestaltung der Zugriffsrechte. Die Aufbewahrungsfristen im Aufbewahrungs-, Archivierungs- und Löschkonzept müssen jedoch in Eigenverantwortung noch überarbeitet werden.

– eUmzug

Die DSA bemängelte, dass das elektronische System eUmzug keine eigentliche Identifizierung verlangt. So ist es möglich, dass eine Person eine andere Person missbräuchlich umziehen lässt, ohne dass dies bei der elektronischen Ummeldung erkannt wird. Damit die Richtigkeit der Registerdaten der Gemeinden, die am Ver-

such von eUmzug teilnehmen, weiterhin gewährleistet bleibt, empfahl die DSA deshalb, die Identitätsprüfung durch die Gemeinde beizubehalten. Gleichwohl setzt die am 1. Februar 2019 in Kraft getretene Versuchsverordnung eUmzug die geltenden Vorschriften zur Prüfung der Identität durch die Gemeindebehörden für die Versuchsphase aus (siehe unten Ziff. 7.2). Die DSA verzichtete auf eine begründete Empfehlung gegen die Inbetriebnahme von eUmzug, da die Richtigkeit der Registerdaten in die Zuständigkeit der Gemeinden und ihrer kommunalen Aufsichtsstellen fällt.

– GELAN

Ergänzend zur Vorabkontrolle des Vorjahres wurde eine mögliche Änderung des Archivierungs- und Vernichtungskonzept zum Agrarinformationssystem GELAN der Kantone Bern (vertreten durch das Amt für Landwirtschaft und Natur), Freiburg und Solothurn GELAN geprüft.

– KIS RSE AG

Die intensive Vorabkontrolle des Klinikinformationssystems (KIS) der RSE AG konnte mit der siebten Stellungnahme der DSA bis auf die Umsetzungsbestätigung der datenschutzrechtlich zwingend erforderlichen Anpassungen abgeschlossen werden. Mit den Verantwortlichen für das System konnte z.B. die Einschränkung vereinbart werden, dass Assistenzärzte (sie leisten Dienste in Burgdorf und Langnau) einen abgeschlossenen Fall via Suchabfrage nur noch sehen, wenn er ihrem eigenen fachlichen Arbeitsbereich angehört.

– Online Umfragetool

Die Vorabkontrolle des Online Umfragetools, das vom KAIO angeboten wird, konnte abgeschlossen werden. Die Nutzung der Anwendung bedingte gewisse Vorgaben an die Benutzer zur Einhaltung des Datenschutzes.

(Zu den ebenfalls einer Vorabkontrolle unterstellten Videoüberwachungen siehe Ziff. 4).

6 Ansichtsäusserungen, Praxis

Folgende Sachverhalte geben einen Einblick in die zahlreichen Anfragen an die DSA:

– Forschungsprojekt Häusliche Gewalt

Im Hinblick auf das Forschungsprojekt «Häusliche Misshandlungen von älteren Personen» der BFH und der Haute Ecole Travail Social Valais erläuterte die DSA auf Einladung der Berner Interventionsstelle gegen häusliche Gewalt die datenschutzrechtlichen Anforderungen. Da sich auch ausserkantonale Behörden und private Organisationen am Projekt beteiligen können sollen, sind für die Datenbearbeitungen die jeweiligen Datenschutzgesetze der Kantone und des Bundes zu beachten.

– Auswirkungen der DSGVO auf Verwaltungsstellen und Gemeinden

Viele verwaltungsinterne und kommunale Anfragen betrafen die Auswirkungen der EU-Datenschutzgrundverordnung 2016/679 (DSGVO). Die DSA erstellte zusammen mit dem Amt für Gemeinden und Raumordnung (AGR) eine Information (BSIG 1/152.04/10.4) als Orientierungshilfe und anfragenden Gemeinden und Verwaltungsstellen Auskünfte erteilt.

– Arbeitsgruppe Prüfgrundlagen für Cloud-Anwendungen des KAIO

Die DSA arbeitete an mehreren Sitzungen der KAIO-Arbeitsgruppe für die Erstellung von einheitlichen kantonalen Prüfgrundlagen für Cloud-Anwendungen mit.

– Motion 142-2018 Gullotti

Zuhanden der Antwort des Regierungsrates auf die Motion «Transparente und präzise Angabe der Religionszugehörigkeit in der Einwohnerkontrolle der bernischen Gemeinden» wies die DSA auf die datenschutzrechtlichen Rahmenbedingungen für das Anliegen der Motion hin.

– Löschen von Daten im Polizeiinformationssystem

Die DSA beantwortete mehrere Fragen von Privatpersonen zur Löschung von Einträgen im Polizeiinformationssystem.

– Mitarbeiterüberwachung

Eine anfragende Institution mit öffentlichem Auftrag im Gesundheitsbereich hatte in ihrem Reglement zur Nutzung elektronischer Kommunikationsmittel für ihre Mitarbeitenden u.a. eine Protokollierung der Nutzung der ICT-Infrastruktur vorgesehen. Die DSA hielt fest, dass eine solche Überwachung einen schweren Eingriff in die Grundrechte darstellt, wofür eine genügende gesetzliche Grundlage erforderlich ist. Ein Reglement reicht hierzu nicht aus, ebenso wenig ein Abstützen einzig auf die gesetzliche Aufgabenerfüllung. Im Rahmen der gesetzlichen Aufgabenerfüllung wären Protokollierungen einzig zur Aufrechterhaltung des technischen Betriebs, zur Behebung von technischen Defekten und dergleichen zulässig.

– Protokolle von Gemeindeversammlungen im Internet

Mehrere Gemeinden stellten der DSA Fragen zur Publikation von Protokollen der Gemeindeversammlung im Internet. Nach dem kantonalen Informationsgesetz sind Gemeindeversammlungen öffentlich. Geht es um die Internetpublikation der betreffenden Protokolle, sind die Vor-

schriften des KDSG und der DSV über die Bekanntgabe von Personendaten ins Ausland zu berücksichtigen, weil im Internet publizierte Daten weltweit abrufbar sind. Eine gesetzliche Grundlage auf kommunaler Ebene ist daher notwendig. Das AGR stellt den Gemeinden auf seiner Homepage dafür eine im Berichtsjahr grundlegend überarbeitete Musterverordnung zur Verfügung. Die zuständige Gemeindebehörde muss sicherstellen, dass die Veröffentlichung im Internet keine besonderen Risiken für die betroffenen Personen verursacht und ihre Persönlichkeit durch die Bekanntgabe ins Ausland nicht schwerwiegend gefährdet wird. Der Schutz überwiegender privater und öffentlicher Interessen sowie die Sperr- bzw. Auskunfts- und Berichtigungsrechte sind zu gewährleisten. Zudem sind die im Internet bekannt gegebenen Informationen technisch so zu markieren, dass den Suchmaschinen vom Indexieren abgeraten wird. Allfällige E-Mail-Adressen dürfen nur in einer Form veröffentlicht werden, die ein Lesen durch Spamroboter verunmöglicht.

– Befunde aus Fahrtüchtigkeitsprüfung

Ein Betroffener erachtete die Zustellung der Befunde aus der ab dem 70. Altersjahr gesetzlich vorgesehenen Fahrtüchtigkeitsprüfung an das Strassenverkehrsamt als Verletzung der ärztlichen Schweigepflicht. Das Strassenverkehrsgesetz sieht allerdings für diesen Fall eine Entbindung vom Berufsgeheimnis vor. Danach dürfen medizinische Befunde dann gemeldet werden, wenn beim Betroffenen verkehrsmedizinisch relevante Erkrankungen oder Zustände festzustellen sind. Die Meldung mittels vorgeschriebenem Formular darf an das die zuständige kantonale Strassenverkehrsbehörde oder an die Aufsichtsbehörde für Ärzte erstattet werden. Als Vertrauensarzt wird nur zugelassen, wer dieses Vorgehen kennt. Das Verfahren beruht nach Ansicht der DSA auf hinreichenden Gesetzesgrundlagen.

– Information der Sozialhilfebehörden

Die DSA wurde angefragt, ob die Fachstelle für kantonale Brückenangebote (Bildungsangebot zwischen Volksschule und Berufslehre) von sich aus Auskünfte zu Einzelpersonen an die Sozialhilfebehörden erteilen dürfen. Laut Sozialhilfegesetz sind die Informationen grundsätzlich bei der betreffenden Person selbst zu beschaffen. Ist dies nicht möglich oder sinnvoll, so müssen die Behörden des Kantons und der Gemeinden Auskünfte erteilen. Sie können von sich aus Informationen an die Sozialhilfebehörden übermitteln, falls sie sichere Kenntnis haben, dass die betroffene Person Sozialhilfe bezieht und die Informationen für die Abklärung der gesetzlichen Ansprüche zwingend erforderlich sind. Ob diese Voraussetzungen zutreffen, ist im Einzelfall zu verifizieren.

– Personendaten in der Störfallvorsorge

Das Aufschalten einer sogenannten Konsultationsbereichskarte mit Namen und Adressen von Firmen im Internet zum Vollzug der eidgenössischen Störfallverordnung (StFV) bedarf einer Grundlage in einer kantonalen Verordnung. Das Bundesrecht reicht dafür nicht aus, andererseits handelt es sich um keinen schweren Grundrechtseingriff, so dass eine Verordnung genügt.

7 Gesetzgebung

7.1 Bundeserlasse und Konkordate

Im Berichtsjahr nahm privatim in den Vernehmlassungen zum Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) und zum Bundesgesetz über Vorläuferstoffe für explosionsfähige Stoffe (VSG) Stellung. Hat sich privatim geäussert oder Stellungnahmen seiner Mitglieder vermittelt, schliesst sich die DSA – wenn nicht spezifisch bernische Gegebenheiten zu berücksichtigen sind – jenen Stellungnahmen an.

7.2 Kantonale Erlasse

Im Berichtsjahr nahm die DSA zu folgenden Erlassen Stellung (Vernehmlassungen und/oder Mitberichte):

– Revision Feuerschutz- und Feuerwehrgesetz (FFG)

Gestützt auf den Hinweis der DSA wird die Gebäudeversicherung auf die Pflicht hingewiesen, in ihrem Datenbanksystem ein Sperrecht nach Art. 13 KDSG zu gewährleisten.

– Revision Personalgesetz (PG)

Die DSA äusserte sich kritisch zur Revision des Personalgesetzes, welche die Grundlagen für den Umgang mit Personendaten schaffen soll, die bei der Nutzung der elektronischen Infrastruktur der Verwaltung (z.B. Telefonie, Clients) anfallen. Sie wies in ihrer Vernehmlassung (https://www.jgk.be.ch > Aufsicht > Datenschutz > Aktuell) darauf hin, dass die vorgeschlagene Regelung den verfassungsrechtlichen Vorgaben für schwere Grundrechtseingriffe nicht genüge. So bemängelte sie, dass das grundsätzliche Verbot von Aufzeichnungen und Auswertungen zum Schutze der Mitarbeitenden aufgeweicht statt geschützt werde. Sie verlangte, dass Behörden, die ausnahmsweise auf die anfallenden Daten zugreifen und sie auswerten dürfen, hinreichend bestimmt bezeichnet und dass die Fristen für die Aufbewahrung und Vernichtung der Daten im Rahmen des jeweiligen Auswertungszweckes ergänzt werden. Zudem solle auf eine umfassende Geltung der Regelung auch

für externe Nutzende der elektronischen Infrastruktur des Kantons verzichtet werden, da dies zu einer wesentlich weitergehenden Datenerhebung über die Einwohnerinnen und Einwohner führen könnte. Eine Auswertung der Nutzung der Webseiten des Kantons darf jedenfalls bereits heute ausschliesslich anonymisiert erfolgen.

– PDSG

Ein Gesetz über zentrale Personendatensammlungen des Kanton Bern (PDSG) soll einerseits das heutige Registerharmonisierungsgesetz ablösen und andererseits eine Rechtsgrundlage für weitere zentrale Personendatensammlungen schaffen. Die DSA wies auf das erhebliche Gefährdungspotential von zentralen Personendatensammlungen hin, wenn von verschiedenen Behörden erhobene Daten von anderen Behörden für neue Zwecke genutzt werden. Die fortschreibende Digitalisierung erlaubt zunehmend die Verknüpfung von Datenbanken sowie den Abruf und die Auswertung einer Vielzahl von Daten (inkl. Profiling). Damit die Bürger für die Behörden nicht zunehmend «gläsern» werden, verlangte die DSA, dass das Bearbeiten insbesondere von besonders schützenswerten Daten hinreichend bestimmt im Gesetz geregelt wird. In der Vernehmlassung (https://www.jgk.be.ch > Aufsicht > Datenschutz > Aktuell.) wies die DSA auf den entsprechenden Verbesserungsbedarf hin.

– Verordnung über den Justizvollzug (JVV) und Weisung AJV zum Löschen und Archivieren von Personen- und weiteren Daten

Die Hinweise der DSA wurden nur teilweise berücksichtigt. Die Polizei- und Militärdirektion hielt den Rahmen aus dem Justizvollzugsgesetz in Verbindung mit dem Datenschutzgesetz sowie die mögliche Kontrolle durch ein Gericht für genügend. Die von der DSA als unverhältnismässig beurteilte dreijährige Aufbewahrungsfrist für elektronische Überwachungsdaten des Electronic Monitoring (siehe auch Ziff. 5) wurde beibehalten.

– Versuchsverordnung eUmzug (eUmzug VV)

Die DSA stellte fest, dass das System eUmzug nicht zu gewährleisten vermag, dass die einen Umzug elektronisch meldende Person identisch ist mit der Person, die umzieht, weil keine formelle Identifikation (z.B. mittels SwissID) erfolgt. So ist es möglich, dass eine Person eine andere Person missbräuchlich «umziehen lässt», was in einem anderen Kanton einmal geschehen ist. Der Antrag der DSA, die Pflicht der Gemeinden, die Identität der Umziehenden mittels des Heimatscheins zu prüfen, nicht aufzuheben, wurde nicht berücksichtigt. Verbesserungen im elektronischen System sind spätestens nach der Versuchsphase bei einer definitiven kantonsweiten Einführung von eUmzug vorzunehmen, weil falsche Daten in den Registern der Einwohnerkontrollen auch in den nachgelagerten Systemen GERES und ZPV zu unrichtigen Daten führen. Vorderhand bleibt es Aufgabe der Gemeinden und deren Datenschutzaufsichtsstellen, ihr Möglichstes zu tun, um die Richtigkeit der Registerdaten zu gewährleisten.

– ASIV

Mit der Verordnung über die Angebote zur sozialen Integration (ASIV) wird die Rechtsgrundlage für den Zugriff auf die GERES-Daten, die für die Ausstellung von Betreuungsgutscheinen nötig sind, durch eine Webapplikation geschaffen. Die DSA empfahl, die Bestimmung für den Zugriff so bestimmt zu formulieren, dass er klar auf die erforderlichen Daten beschränkt ist.

– Verordnung über das Veranlagungsverfahren (VVV)

Eine Änderung der Verordnung über das Veranlagungsverfahren ermöglicht es den Steuerpflichtigen, ab 1. Januar 2019 ihre Steuererklärung elektronisch freizugeben. Die DSA verlangte, dass das elektronische System sicherstellt, dass eine elektronische Freigabe ausschliesslich durch die eindeutig identifizierten Steuerpflichtigen erfolgt, worauf die Steuerverwaltung den Prozess eingehend beschrieb. Dieser stützt sich für die Identifikation – wie bereits heute für TaxMe-Online – auf die im Zentralen Personenverzeichnis (ZPV) amtlich hinterlegten Adresse. Die Steuerpflichtigen werden über die nötigen Identifizierungsschritte informiert werden.

– Gesetz über die sozialen Leistungsangebote (SLG)

In der Vernehmlassung (https://www.jgk.be.ch > Aufsicht > Datenschutz > Aktuell) äusserte sich die DSA zur Aufhebung des Schutzes des Sozialhilfegeheimnisses für den Bereich der individuellen Sozialhilfe (mit Ausnahme des Bereichs erwachsener Menschen mit Behinderung). Sie hielt fest, dass das Sozialhilfegeheimnis bereits heute derart «durchlöchert» sei, dass eine Verringerung des Kreises der durch das Sozialhilfegeheimnis geschützten Personen kaum mehr ins Gewicht falle. Durch eine indirekte Änderung des Sozialhilfegesetzes (SHG) soll das Sozialhilfegeheimnis sogar noch weiter ausgehöhlt werden, so dass sich die Frage stellt, inwieweit das Geheimnis überhaupt noch einen Schutz bietet, der über jenen für besonders schützenswerte Personendaten hinausgeht.

7.3 Register Datensammlungen

Im Berichtsjahr wurden laufend weitere Einträge in das Register der Datensammlung aufgenommen. Für die Abgabe an das Staatsarchiv wur-

den Verbesserungen an der Registerdatenbank und am Formular vorgenommen.

8 Aufsichts- und Justizentscheide

– BE-GEVER

Siehe zu den begründeten Empfehlungen und Beschwerden betreffend BE-GEVER oben Ziff. 5.1.

– Verwaltungsbeschwerde zur Aufbewahrungsdauer und Bekanntgabe von Log-Daten

Mit Beschwerde vom 26. Juli 2018 an die FIN rügte die DSA eine ablehnende Verfügung des KAIO betreffend die Vorabkontrolle zur Plattform DDI-Services, welche die drei Basisdienste Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) und IP Address Management (IPAM) zusammenfassen soll. Die Dienste bilden die Grundlage für die gesamte Kommunikation über ein IP-basiertes Netzwerk. Bei der (teils auch privaten) Nutzung des Internet durch die Mitarbeitenden aller kantonaler Behörden entstehen Logdaten. Die DSA verlangte, mangels einer gesetzlichen Grundlage sei für Logdaten eine Höchstaufbewahrungsfrist von sechs Wochen vorzugeben. Eine längere Dauer dürfe dort vorgesehen werden, wo innerhalb der sechswöchigen Frist Daten in einem eingeleiteten Verfahren Verwendung fänden. Für die Bekanntgabe der Logdaten an Dritte sei generell und besonders für Strafverfolgungsuntersuchungen vorzugeben, dass diese nur unter Wahrung der Zustimmungsrechte der berechtigten Stellen erfolgen dürften. Mit der Aufzeichnung und Auswertung der Randdaten, die bei der Nutzung der DDI-Services anfallen, werden auch besonders schützenswerte Personendaten bearbeitet. Das Aufbewahren und Auswerten dieser Personendaten führt regelmässig zu einem schweren Eingriff in das Grundrecht auf Datenschutz der betroffenen Mitarbeitenden. Fehlt eine Regelung dazu in einem formellen Gesetz, ist das Bearbeiten, soweit es nicht zur Erfüllung einer gesetzlichen Aufgabe zwingend erforderlich ist, nicht zulässig. Der Entscheid über eine Bekanntgabe solcher Daten an Dritte steht den Behörden zu, bei denen die Daten anfallen.

– Urteil des Verwaltungsgerichts vom 31. Januar 2018 (100.2017.72U)

Das Verwaltungsgericht trat auf eine Beschwerde nicht ein, welche die DSA gegen eine Verfügung der Staatskanzlei erhoben hatte. Die DSA hatte sich auf den Standpunkt gestellt, dass die Bearbeitung von Personendaten im Rahmen eines Pilotbetriebs zur neuen Geschäftsverwaltung BE-GEVER nicht datenschutzkonform erfolge, solange weder eine Zwei-Faktoren-Authentifizierung noch eine Ablage von digital signierten Dokumenten vorgesehen sei. Deshalb habe die Staatskanzlei die Bearbeitung von Personendaten weiterhin papiergebunden zu dokumentieren. Das Gericht stellte zunächst fest, dass die Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Richtigkeit) betreffend Personendaten durchaus ein Anliegen des Datenschutzes darstelle und daher Gegenstand einer Empfehlung der DSA sein könne. Jedoch verlange die DSA nur die papiergebundene Dokumentation der Datenbearbeitungen und keine Behebung von Sicherheitsdefiziten im GEVER-System, weshalb sich das Gericht im Urteilsdispositiv auch nicht zu den sicherheitsmässigen Anforderungen an jenes System äussern könne. Selbst eine Gutheissung der Beschwerde würde die Mängel nicht beseitigen. Deshalb habe die DSA kein schutzwürdiges Interesse, so dass auf die Beschwerde nicht einzutreten sei. Immerhin wies das Gericht abschliessend darauf hin, dass im Hinblick auf weitere Verfahren gestützt auf eine Risikoanalyse aufzuzeigen sei, welche Sicherheitsmassnahmen verhältnismässig seien bzw. weshalb auf weitergehende Sicherungselemente verzichtet werden könne. Dabei sei von Interesse «warum im Kanton Bern die Einmal-Anmeldung für den Zugang zur elektronischen Geschäftsverwaltung genügen soll, wogegen die GEVER-Systeme im Bund gemäss den Vorgaben über die Informatiksicherheit mit einer Zwei-Faktoren-Authentifikation zu führen sind» (E. 4.2).

– Urteil des Verwaltungsgerichts vom 6. Dezember 2018 (100.2017.133U)

Das Verwaltungsgericht wies eine Beschwerde ab, welche die DSA gegen einen Entscheid der Finanzverwaltung erhoben hatte. Seit 2016 ist es den Steuerpflichtigen nicht mehr möglich, nur Rechnungen elektronisch in ihr e-Banking Portal sowie Verfügungen und Entscheide auf dem Postweg zu erhalten; stattdessen müssen sie für alles den gleichen Weg wählen. Die DSA beanstandete dies und stellte die Freiwilligkeit der Zustimmung zur elektronischen Zustellung auch von Verfügungen und Entscheide als nicht datenschutzkonform in Frage. Das Gericht wies die Beschwerde ab. Nach einer ausführlichen Analyse zur Freiwilligkeit einer Einwilligung gelangte es zum Schluss, dass eine Einwilligung nach herrschender Lehre und Praxis nur dann nicht freiwillig ist, «wenn die Nachteile, die bei einer Ablehnung drohen, in keinem Zusammenhang mit der Datenbearbeitung und der damit verfolgten Zielsetzung stehen oder unverhältnismässig sind» (E 3.7). Zusammenfassend ergebe sich, dass «die Nachteile, die die steuerpflichtige Person auf sich nimmt, wenn sie der elektronischen Eröffnung von Verfügungen und Entscheiden nicht zustimmt – nämlich die postalische Zustellung von Steuerrechnungen – mit

dieser zusammenhängen und zumutbar sind. Die Einwilligung in die Eröffnung von Verfügungen und Entscheiden auf dem Weg der E-Rechnung erfolgt damit freiwillig und gültig» (E 4.2). Aus der Tatsache, dass heute weniger Steuerpflichtige die E-Rechnung wählen, lasse sich nicht schliessen, «dass diejenigen, die sich für die E-Rechnung und damit das 'Gesamtpaket' entschieden haben, ihre Entscheidung nicht frei gefällt haben. Soweit aus diesen Zahlen überhaupt etwas gewonnen werden kann, dann wohl, dass die Steuerpflichtigen, die sich (neu) gegen die E-Rechnung entschieden haben, die mit einer postalischen Zustellung verbundenen allfälligen Nachteile in Kauf genommen und diese folglich als zumutbar erachtet haben» (E 4.3).

– Zuständigkeit der DSA für die IV-Stellen

Ein Bürger hatte die IV-Stelle des Kantons Solothurn gestützt auf die kantonale Öffentlichkeitsgesetzgebung um Auskunft darüber ersucht, in wie vielen Fällen zwei Ärzte in ihren insgesamt 109 Gutachten zuhanden der IV in den Jahren 2012 bis 2014 eine Arbeitsunfähigkeit von mehr als 40 Prozent attestiert hatten und in wie vielen Fällen daraus eine leistungsbegründende Invalidität abgeleitet worden war. Die solothurnische Behörde hatte das Gesuch abgelehnt und die daraufhin beigezogene kantonale Datenschutzaufsichtsstelle für unzuständig gehalten. Das solothurnische Verwaltungsgericht und danach auch das Bundesgericht erkannten, dass die IV-Stellen datenschutzrechtlich keine Bundesorgane seien, obwohl sie solchen nahekommen und Bundesrecht vollziehen würden, weshalb sie nicht dem Datenschutzgesetz des Bundes unterstünden. Auch beim Öffentlichkeitsgesetz habe der Bundesgesetzgeber die IV-Stellen nicht dem Bundesrecht unterstellen wollen. Aus dem im Berichtsjahr ergangenen Urteil des Bundesgerichts ergibt sich nun klar, dass die IV-Stellen dem entsprechenden kantonalen Recht und damit auch den kantonalen Datenschutzaufsichtsstellen unterstehen (Urteil vom 27. Juni 2018 [1C 461/2017]).

9 Gemeinderechtliche Körperschaften

Im Rahmen ihrer Oberaufsicht beriet die DSA kommunale Aufsichtsbehörden auf Anfrage, u.a. die Aufsichtsstelle der Gemeinde Ostermundigen zu Datenlieferungen an iCampus (Mustervereinbarung), die Aufsichtsstelle der röm.-kath. Gesamtkirchgemeinde Bern zu Fragen zu ihrer geplanten Informatikstrategie sowie zahlreiche Gemeinden betreffend die Auswirkungen der EU DSGVO (siehe oben Ziff. 6).

10 Berichtspunkte der Vorjahre

(3: Nachbetreuungen zu den 2017 vorgenommenen Kontrollhandlungen, 5: weitergeführte Vorabkontrollen, 8: Urteile des Verwaltungsgerichts zu den Verwaltungsgerichtsbeschwerden betreffend BE-GEVER und die elektronische Zustellung von Verfügung und Entscheide der Steuerverwaltung).

11 Antrag

Dem Regierungsrat und dem Grossen Rat wird nach Artikel 37 des Datenschutzgesetzes beantragt, vom Bericht Kenntnis zu nehmen.

19. März 2019

Der Datenschutzbeauftragte: *Ueli Buri*