100.2017.72U publiziert in BVR 2018 S. 189
DAM/RAP

Verwaltungsgericht des Kantons Bern
Verwaltungsrechtliche Abteilung

Urteil vom 31. Januar 2018

Verwaltungsrichter Burkhard, Abteilungspräsident
Verwaltungsrichter Daum und Häberli
Gerichtsschreiber Bieri

Datenschutzaufsichtsstelle des Kantons Bern
Münstergasse 2, 3011 Bern

Beschwerdeführerin

gegen

Staatskanzlei des Kantons Bern
Postgasse 68, 3000 Bern 8

betreffend Datenschutz; Pilotbetrieb Digitale Geschäftsverwaltung und Archivierung in der Staatskanzlei (Verfügung der Staatskanzlei des Kantons Bern vom 3. Februar 2017; 473341 / 2015.STA.23086)

Sachverhalt:

A.

Der Kanton Bern beabsichtigt, den Umgang mit Informationen in der Verwaltung zu modernisieren. Dazu wurde das Programm «Digitale Geschäftsverwaltung und Archivierung» (DGA) entwickelt. Es sieht vor, in der Zentralverwaltung flächendeckend ein Informatiksystem zur digitalen Geschäftsverwaltung (BE-GEVER) und Archivierung (eArchiv) einzuführen. Der Regierungsrat genehmigte am 24. Juni 2014 die Realisierung des Programms; am 1. September 2014 beschloss der Grosse Rat dafür den Rahmenkredit. Der Evaluation und Einführung einer elektronischen Geschäftsverwaltungssoftware im Rahmen von BE-GEVER diente das Teilprojekt «Basisinfrastruktur» (BI) unter der Verantwortung des Amts für Informatik und Organisation (KAIO). Seit Herbst 2016 wurde in der Staatskanzlei (STA) und im KAIO als Pilotversuch die Software «CMI AXIOMA» zur Geschäftsverwaltung eingesetzt. Im Frühjahr 2017 endete die Phase des Pilotbetriebs in diesen beiden Verwaltungseinheiten. Das Produkt «CMI AXIOMA» wird dort nunmehr definitiv eingesetzt und im Zeitraum 2017-2021 als Teil von direktionsspezifischen Einführungsprojekten sukzessive in den einzelnen Direktionen eingeführt; als letzte Amtsstelle soll die Kantonspolizei auf das neue System umstellen.

B.

Am 9. Januar 2017 gelangte die Datenschutzaufsichtsstelle des Kantons Bern (nachfolgend: Aufsichtsstelle) an die STA mit der Empfehlung bzw. dem Antrag, diese habe ihr Handeln, soweit im Pilotbetrieb BE-GEVER Personendaten bearbeitet werden, weiterhin papiergebunden zu dokumentieren. Zur Begründung brachte sie im Wesentlichen vor, es seien keine angemessenen Informationssicherheitsmassnahmen ergriffen worden. Namentlich sei für die Anmeldung am System weder eine Zwei-Faktoren-Authentifizierung vorgesehen noch würden die elektronisch abgelegten Dokumente digital signiert, um ihre Authentizität sicherzustellen. Mit Verfügung vom 3. Februar 2017 gab die STA dem Antrag nicht statt.

C.

Dagegen hat die Aufsichtsstelle am 6. März 2017 Verwaltungsgerichtsbeschwerde erhoben mit dem Rechtsbegehren, die angefochtene Verfügung sei aufzuheben. Mit Vernehmlassung vom 3. April 2017 hat die STA beantragt, auf die Beschwerde sei nicht einzutreten; eventuell sei ihr eine neue Frist von mindestens 60 Tagen zur Stellungnahme in der Sache anzusetzen. Mit Verfügung vom 6. April 2017 hat der Abteilungspräsident das Verfahren wie von der STA beantragt auf die Frage der Beschwerdebefugnis beschränkt. Mit Stellungnahme vom 5. Mai 2017 hat die Aufsichtsstelle beantragt, auf ihre Beschwerde sei einzutreten; das Eventualbegehren der STA sei abzuweisen.

Mit Verfügung vom 28. Juli 2017 hat der Instruktionsrichter die Beschränkung des Verfahrens aufgehoben. Die STA hat mit Eingabe vom 21. August 2017 beantragt, auf die Beschwerde sei nicht einzutreten, eventuell sei sie abzuweisen. Die Aufsichtsstelle hat mit ihrer Stellungnahme vom 14. September 2017 an den gestellten Anträgen festgehalten. Die STA hat sich am 27. Oktober 2017 nochmals zur Sache geäussert.

D.

Im Zug der direktionsspezifischen Einführung des Produkts «CMI AXIOMA» hat die Aufsichtsstelle weitere Empfehlungen abgegeben. Das betrifft einerseits das Generalsekretariat und die Finanzverwaltung der Finanzdirektion (FIN; Empfehlungen vom 18.10.2017) und andererseits die Steuerverwaltung und das Personalamt, die ebenfalls zur FIN gehören (Empfehlungen vom 30.11.2017). Mit Verfügungen vom 7. November und 21. Dezember 2017 stellte die FIN in Aussicht, über die Umsetzung der Empfehlungen in der Sache zu einem späteren Zeitpunkt mit separater Verfügung zu entscheiden, sobald der «rechtskräftige Endentscheid» im vorliegenden Verfahren ergangen sei. Gegen beide Verfügungen hat die Aufsichtsstelle je Verwaltungsgerichtsbeschwerde erhoben. Die Verfahren 100.2017.320 und 100.2018.16 sind gegenwärtig hängig.

Erwägungen:

1.

1.1 Das Verwaltungsgericht ist zur Beurteilung der Beschwerde als letzte kantonale Instanz gemäss Art. 74 Abs. 1 i.V.m. Art. 76 und 77 des Gesetzes vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG; BSG 155.21) zuständig (vgl. auch hinten E. 2.2).

1.2 Ausgangspunkt der hier zu beurteilenden Streitigkeit ist die Empfehlung bzw. der Antrag der Aufsichtsstelle, die STA habe ihr Handeln weiterhin papiergebunden zu dokumentieren, soweit im Pilotbetrieb BE-GEVER Personendaten bearbeitet werden. Die Vorinstanz hat mit der angefochtenen Verfügung entschieden, diesem Begehren nicht stattzugeben (vorne Bst. B). Sie stellt vor Verwaltungsgericht die Behandlung der Beschwerde in Frage, weil die Aufsichtsstelle nur die Aufhebung der angefochtenen Verfügung verlangt und keinen reformatorischen Antrag stellt (vorne Bst. C). Dem kann nicht gefolgt werden. Mit dem Begehren um Aufhebung der abschlägigen Verfügung der STA will die Aufsichtsstelle erreichen, dass ihrer ursprünglichen Empfehlung entsprochen wird. Damit hat sie den Verfahrensgegenstand festgelegt, der zudem den Rahmen des Streitgegenstands im Beschwerdeverfahren vorgibt (vgl. Vortrag des Regierungsrats betreffend Änderung des Datenschutzgesetzes, in Tagblatt des Grossen Rates 2008, Beilage 6 [nachfolgend: Vortrag Revision KDSG], S. 14; allgemein zum Begriff des Streitgegenstands statt vieler BVR 2017 S. 514 E. 1.2 mit weiteren Hinweisen). Die Pflicht zur Umsetzung der Empfehlung besteht, sofern die Verwaltung keine ablehnende Verfügung erlässt (vgl. dazu Vortrag Revision KDSG, S. 10). Bei dieser Ausgangslage steht fest, dass der Aufhebungsantrag die (reformatorische) Rechtsfolge mitumfasst, der ursprünglich abgegebenen Empfehlung sei Folge zu leisten.

2.

2.1 Die Beschwerdebefugnis der Aufsichtsstelle lässt sich nicht auf die allgemeine Legitimationsregelung von Art. 79 Abs. 1 VRPG stützen (vgl. BVR 1990 S. 258 E. 3 betreffend ein kantonales Amt; ferner BGE 123 II 542 E. 2f und g für den damaligen Eidgenössischen Datenschutzbeauftragten). Es fragt sich jedoch, ob ihr ein besonderes Beschwerderecht im Sinn von Art. 79 Abs. 2 VRPG zukommt. Danach ist zur Verwaltungsgerichtsbeschwerde jede andere Person, Organisation oder Behörde befugt, die durch Gesetz oder Dekret dazu ermächtigt ist.

2.2 Gemäss Art. 35 Abs. 5 des Datenschutzgesetzes vom 19. Februar 1986 (KDSG; BSG 152.04) kann die Aufsichtsstelle die Verfügung anfechten, mit der die verantwortliche Behörde ihrem Antrag zur Beseitigung von Verstössen und Mängeln nach Art. 35 Abs. 4 und 3 KDSG nicht oder nur zum Teil stattgegeben hat; Verfahren und Zuständigkeit richten sich nach Art. 26 KDSG, d.h. für das Verfahren und den Rechtsschutz gelten die Bestimmungen der für das betreffende Rechtsgebiet anwendbaren Verfahrensordnung, soweit das KDSG nichts anderes bestimmt. In Verfahren vor den Verwaltungsjustizbehörden ist die Aufsichtsstelle damit gestützt auf Art. 65 Abs. 2 bzw. Art. 79 Abs. 2 VRPG i.V.m. Art. 35 Abs. 5 und Art. 26 KDSG spezialgesetzlich zur Beschwerde befugt (sog. Behördenbeschwerde; Ivo Schwegler, Datenschutzrecht, in Müller/Feller [Hrsg.], Bernisches Verwaltungsrecht, 2. Aufl. 2013, S. 342 ff., 371 N. 127 mit Hinweis auf die Materialien).

2.3 Die STA stellt sich auf den Standpunkt, das Rechtsmittel werfe nicht Fragen des Datenschutzrechts auf; vielmehr gehe es um die «Nachvollziehbarkeit des Verwaltungshandelns». Angesprochen seien damit vorab Vorgaben der Archivgesetzgebung. In diesem Bereich sei die Aufsichtsstelle nicht befugt, Empfehlungen abzugeben und abschlägige Verfügungen nach Massgabe des KDSG mit Behördenbeschwerde anzufechten.

2.4 Inwieweit eine Behörde zur Beschwerde ermächtigt ist, beurteilt sich regelmässig nach Massgabe des entsprechenden Sacherlasses (vgl. BVR 1990 S. 258 E. 5; BGE 134 II 124 E. 2.6.3). Zu klären ist damit der Anwendungsbereich des KDSG im vorliegenden Fall. – Das erwähnte Ge-

setz dient dem Schutz von Personen vor missbräuchlicher Datenbearbeitung durch Behörden (Art. 1 KDSG). Es gilt grundsätzlich für jedes Bearbeiten von Personendaten durch Behörden (Art. 4 Abs. 1 KDSG). Zu den Behörden in diesem Sinn zählen Amtsstellen des Staates (heute: Kantons) und der Gemeinden mit ihren Mitarbeiterinnen und Mitarbeitern (Art. 2 Abs. 6 Bst. a KDSG). Personendaten sind Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person (Art. 2 Abs. 1 KDSG); gewisse gesetzlich umschriebene Angaben gelten als besonders schützenswerte Personendaten (Art. 3 KDSG). Als Datensammlung gilt jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach den betroffenen Personen erschliessbar sind (Art. 2 Abs. 2 KDSG). Das «Bearbeiten» umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten (Art. 2 Abs. 4 KDSG).

2.5 Die STA stellt zu Recht nicht in Abrede, dass BE-GEVER Personendaten beinhaltet, die unter das KDSG fallen und im Rahmen der elektronischen Geschäftsverwaltung bearbeitet werden. Ihr Hinweis auf die Archivierungsgesetzgebung führt nicht weiter, ist als Bearbeiten von Personendaten doch nach Art. 2 Abs. 4 KDSG namentlich auch das «Aufbewahren» aufzufassen. Erst wenn solche Daten aus dem Bearbeitungsprozess ausscheiden, dürfen sie archiviert werden (vgl. Art. 19 KDSG i.V.m. Art. 14 des Gesetzes vom 31. März 2009 über die Archivierung [ArchG; BSG 108.1]; Ivo Schwegler, a.a.O., S. 361 N. 93). In den Schutzbereich des KDSG fallen alle Phasen der Datenbearbeitung (BVR 2009 S. 49 E. 4.1). Welche Mittel dabei verwendet und welche Verfahren angewendet werden, ist nicht entscheidend, wie die Parallelbestimmung von Art. 3 Bst. e des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) ausdrücklich festhält (vgl. dazu BGer 2C_437/2011 vom 24.2.2012 E. 2.3.1; ferner auch Rainer J. Schweizer, in St. Galler Kommentar zur BV, 3. Aufl. 2014, Art. 13 N. 74). Neben dem manuellen kommt deshalb auch das elektronische Bearbeiten in Betracht (vgl. David Rosenthal, in Rosenthal/Jöhri [Hrsg.], Handkommentar zum Datenschutzgesetz, 2008, Art. 3 N. 66).

2.6 Wer Personendaten bearbeitet, sorgt für ihre Sicherung (Art. 17 KDSG). Die Datensicherheit ist ein Kernelement jeglichen Bearbeitens von Personendaten (Waldmann/Oeschger, Datenbearbeitung durch kantonale Organe, in Eva Maria Belser et al. [Hrsg.], Datenschutzrecht, 2011, S. 765 ff., 816 f. N. 57; Bruno Baeriswyl, in Handkommentar DSG, 2015, Art. 7 N. 1). Dementsprechend überwacht die Aufsichtsstelle unter anderem die Datensicherung (Art. 34 Abs. 1 Bst. h KDSG). Inhaltlich wird dieser Grundsatz in Art. 4 ff. der Datenschutzverordnung vom 22. Oktober 2008 (DSV; BSG 152.040.1) näher ausgeführt. Die verantwortliche Behörde, die Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt gemäss Art. 4 Abs. 1 DSV mit technischen und organisatorischen Massnahmen für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten; sie schützt die Systeme gegen folgende Risiken: unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl oder widerrechtliche Verwendung, sowie unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. Insbesondere bei der elektronischen Bearbeitung von Personendaten hat eine Zugangskontrolle zu erfolgen, d.h. unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren (Art. 5 Abs. 1 Bst. a DSV). Es sind sodann weitere Kontrollmechanismen vorzusehen (z.B. Personendatenträger-, Speicher-, Benutzer-, Zugriffs- und Eingabekontrolle; Art. 5 Abs. 1 Bst. b und e-h DSV). Zum Schutz der Personendaten kommen dabei unter anderem technische, d.h. mechanische und elektronische Schutzvorkehren in Betracht (z.B. Einschliessen von Akten, Schutz durch Passwörter und Verschlüsselung, Erstellen von Sicherungskopien usw.), andererseits organisatorische Massnahmen (Zugriffsbeschränkungen, Klassifizierung, Definition der Arbeitsabläufe usw.; Ivo Schwegler, a.a.O., S. 352 N. 70; vgl. als Beispiel VGE 2012/330 vom 15.8.2013 betreffend Benutzerberechtigungskonzept eines Klinikinformationssystems).

2.7 Wie sich aus diesen Rechtsgrundlagen ergibt, verfolgt die Aufsichtsstelle durchaus Anliegen des Datenschutzes, wenn sie geltend macht, die Datensicherheit sei mit BE-GEVER nur unzulänglich gewährleistet (Verzicht auf Zwei-Faktoren-Authentifizierung und digitale Signatur). Das zeigt nicht zuletzt die angefochtene Verfügung, hat die STA doch einschlägige

datenschutzrechtlichen Vorschriften – namentlich Art. 4 DSV – thematisiert und angewendet, um zu beurteilen, ob der Empfehlung der Aufsichtsstelle stattzugeben sei oder nicht. Sie anerkennt damit letztlich selber, dass hier nicht nur die allgemeine Nachvollziehbarkeit des staatlichen Handelns zur Diskussion steht. Nicht zu überzeugen vermag sodann der Einwand der STA, es sei nicht ersichtlich, welcher Mehrwert für den Datenschutz mit der Papieraktenführung erzielt werden könne, wie sie die Aufsichtsstelle verlangt. Damit ist nicht der Anwendungsbereich des KDSG angesprochen, sondern vielmehr die Frage, welche Massnahmen ergriffen werden müssen, um die nach Ansicht der Aufsichtsstelle mangelhafte Datensicherheit zu gewährleisten. Auf diesen Problemkreis wird noch zurückzukommen sein.

2.8 Die Aufsichtsstelle ist somit grundsätzlich befugt, gegen die Verfügung der STA vom 3. Februar 2017 Behördenbeschwerde zu führen (Art. 79 Abs. 2 VRPG i.V.m. Art. 35 Abs. 5 und Art. 26 KDSG).

3.

3.1 Die Behördenbeschwerde setzt abweichend von der allgemeinen Legitimationsregelung gemäss Art. 79 Abs. 1 Bst. c VRPG grundsätzlich nicht voraus, dass ein schutzwürdiges Interesse im Sinn der materiellen Beschwer dargetan wird (vgl. BGE 136 II 359 E. 1.2, 129 II 1 E. 1.1; BGer 3.11.1997, in ZBl 1999 S. 64 E. 1c; VGE 19931 vom 19.10.2001 E. 1b; Merkli/Aeschlimann/Herzog, Kommentar zum bernischen VRPG, 1997, Art. 65 N. 19). Immerhin darf die Beschwerde nicht nur der Behandlung einer vom konkreten Fall losgelösten abstrakten Frage des objektiven Rechts dienen. Sie hat sich vielmehr auf konkrete Probleme eines tatsächlich bestehenden Einzelfalls zu beziehen, die von einer gewissen Aktualität und (wenigstens potenziellen) Relevanz sind (vgl. für das Beschwerderecht von Bundesbehörden BGE 135 II 338 E. 1.2.1, 128 II 193 E. 1; VGE 2015/141 vom 11.6.2015 E. 1.2.1; Kölz/Häner/Bertschi, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 3. Aufl. 2013, N. 980; Marantelli-Sonanini/Huber, Praxiskommentar VwVG, 2. Aufl. 2016, Art. 48 N. 43). In diesem Sinn muss die Behörde eine vernünftige Veranlassung

zur Beschwerdeführung haben (BGE 114 V 239 E. 3b mit Hinweis auf Fritz Gygi, Bundesverwaltungsrechtspflege, 2. Aufl. 1983, S. 164).

3.2 Die Aufsichtsstelle stellt in ihrer Beschwerde Fragen der Datensicherheit beim Betrieb von BE-GEVER in den Vordergrund; sie verfolgt damit Anliegen des Datenschutzes (vorne E. 2), mithin ein öffentliches Interesse. Im Einzelnen kritisiert sie die verwendete Authentifizierungsmethode, wonach sich die Benützerinnen und Benützer mit ihrem individuellen Windows-Passwort an ihrem Arbeitsplatz und damit auch für das System BE-GEVER anmelden (Prinzip der Einmal-Anmeldung, sog. Single Sign-on). Datenschutzrechtlich zwingend sei eine Zwei-Faktoren-Authentifizierung, bei der die Identität der Benützerin oder des Benützers mittels der Kombination zweier unterschiedlicher und unabhängiger Faktoren nachgewiesen wird (z.B. Passwort und Code, der per SMS übermittelt wird). Weiter bemängelt die Aufsichtsstelle, dass abgelegte Dokumente nicht digital signiert werden. Eine solche Signatur dient dazu, die Echtheit eines Dokuments bzw. der elektronisch abgelegten Daten sowie die Identität der oder des Unterzeichneten zu überprüfen.

3.3 Das vorliegende Verfahren bezieht sich auf den Pilotbetrieb von BE-GEVER in der STA, der im Frühjahr 2017 zu Ende ging. Insofern liegt nicht auf der Hand, dass die von der Aufsichtsstelle thematisierten Fragen noch aktuell sind. Das neue Geschäftsverwaltungssystem soll nun schrittweise in der gesamten Verwaltung eingeführt werden (vorne Bst. A). Hinsichtlich der Datensicherheit sind – soweit hier interessierend – keine Änderungen vorgesehen, d.h. es wird weiterhin auf eine Zwei-Faktoren-Authentifizierung und eine digitale Signatur verzichtet. Die aufgeworfenen Sicherheitsaspekte bleiben so gesehen über die Pilotphase hinaus aktuell und für den Betrieb von BE-GEVER relevant.

3.4 Prozessual von Bedeutung ist allerdings, dass die Aufsichtsstelle im vorliegenden Verfahren nicht verlangt, die Software «CMI AXIOMA» sei entsprechend den datenschutzrechtlichen Anforderungen auszugestalten. Auf ein solches Begehren hat sie vielmehr verzichtet. Wie bereits mit ihrer ursprünglichen Empfehlung beantragt sie lediglich, das Handeln der STA sei weiterhin papiergebunden zu dokumentieren. Zwar mag die Aktenführung in Papierform dazu beitragen, die Richtigkeit der Personendaten zu

sichern; kommt es im elektronischen Datenbestand der Geschäftsverwaltung zu unrechtmässigen Veränderungen, sind die ursprünglichen Informationen immer noch in Papierform vorhanden. An den aus Sicht der Aufsichtsstelle bestehenden Sicherheitsdefiziten ändert sich damit jedoch nichts; die angeblichen Mängel bleiben bestehen, selbst wenn dem Antrag der Aufsichtsstelle voll entsprochen würde. Das Verwaltungsgericht kann sich dazu nicht im Urteilsdispositiv äussern (vgl. zum Streitgegenstand vorne E. 1.2); nur dispositivmässig getroffene Anordnungen werden aber rechtskräftig und verbindlich (vgl. statt vieler BVR 2016 S. 237 E. 4.1 mit Hinweisen). Es besteht demnach kein Anlass, auf die sicherheitsmässigen Anforderungen an die Geschäftsverwaltungs-Software einzugehen, die sich aus dem Datenschutzrecht ergeben; mangels verbindlicher Klärung der Rechtslage käme dem verwaltungsgerichtlichen Erkenntnis keine aktuelle und wenigstens potenziell relevante Bedeutung zu.

3.5 Das Begehren um papiergebundene Aktenführung muss in engem Zusammenhang gesehen werden mit den Anforderungen an die Datensicherheit für BE-GEVER. Das zeigt deutlich das Vorgehen der Aufsichtsstelle, das den Verfahren 100.2017.320 und 100.2018.16 zugrunde liegt. Dort hat sie gegenüber der Verwaltung beantragt, es sei raschmöglichst dafür zu sorgen, dass die Anmeldung an BE-GEVER über eine dem Stand der Technik genügende Zwei-Faktoren-Authentifizierung erfolge; bis dahin seien alle Unterlagen, die in BE-GEVER eingebunden werden, als digital signierte Unterlagen aufzunehmen. Soweit den Mitarbeiterinnen und Mitarbeitern die für ein digitales Signieren erforderlichen technischen Mittel fehlen, sei ihr Handeln bis zur Einführung einer Zwei-Faktoren-Authentifizierung weiterhin papiergebunden zu dokumentieren. Letztere Empfehlung versteht die Aufsichtsstelle damit als einstweilige bzw. vorübergehende Massnahme bis zur Anpassung der Software an die datenschutzrechtlichen Sicherheitsanforderungen. Unter diesen Umständen rechtfertigt es sich nicht, im vorliegenden Verfahren isoliert über diesen Antrag zu entscheiden. Zum einen müsste für eine vertiefte Prüfung auf die aufgeworfenen Sicherheitsfragen eingegangen werden, die hier jedoch nicht Thema einer Empfehlung der Aufsichtsstelle und auch nicht Streitgegenstand bilden (E. 3.4 hiervor) und für deren Beurteilung die Akten noch unvollständig sind (E. 3.6 hiernach und E. 4). Es liegt daher näher, die Datensicherheit in

einer Gesamtschau zu beurteilen. Mit dieser Aufgabe wird sich voraussichtlich die FIN zu befassen haben, zumal das Verwaltungsgericht die Empfehlungen der Aufsichtsstelle in den beiden erwähnten weiteren Beschwerdeverfahren nicht als erste und einzige kantonale Instanz in der Sache beurteilen wird (vorne Bst. D). Zum anderen vermag die Aufsichtsstelle nicht aufzuzeigen, dass die geltend gemachten Sicherheitsdefizite derart gravierend sein sollen, dass mit einer umgehenden Anordnung parallel zur elektronischen weiterhin auch eine papiergebundene Aktenführung verlangt werden müsste. In der Verwaltung dürften denn auch schon seit längerer Zeit, mithin unabhängig vom Projekt BE-GEVER, zahlreiche Datensammlungen existieren, die nur elektronisch bzw. digital geführt werden und auf die mit der Einmal-Anmeldung zugegriffen werden kann.

3.6 Auf die Beschwerde ist somit mangels schutzwürdigen Interesses der Aufsichtsstelle nicht einzutreten. Bei diesem Ergebnis sind weitere Beweismassnahmen zu Fragen, die sich in der Sache stellen, entbehrlich. Namentlich kann darauf verzichtet werden, weitere Unterlagen beizuziehen bzw. die Akten ergänzen zu lassen, wie die Aufsichtsstelle dies verlangt. Der entsprechende Beweisantrag wird abgewiesen. Zudem besteht kein Anlass, der STA Gelegenheit zu geben, sich weitergehend zu materiellen Aspekten der Angelegenheit äussern zu können.

4.

4.1 Bei diesem Ergebnis hat sich das Verwaltungsgericht in der Sache nicht zu äussern. Im Hinblick auf die beiden Verfahren vor der FIN ist immerhin Folgendes in Erinnerung zu rufen: Welche technischen und organisatorischen Massnahmen zum Schutz der mit BE-GEVER bearbeiteten elektronischen Daten ergriffen werden müssen, beurteilt sich massgeblich nach dem Grundsatz der Verhältnismässigkeit (Art. 5 Abs. 2 der Bundesverfassung [BV; SR 101]; vgl. zum Bundesrecht etwa Hussein Noureddine, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in Nicolas Passadelis et al. [Hrsg.], Handbücher für die Anwaltspraxis: Datenschutzrecht, 2015, S. 73 ff., 98 N. 3.102). Dementsprechend müssen die Massnahmen nach Art. 4 Abs. 2 DSV angemessen sein; sie tragen insbe-

sondere folgenden Kriterien Rechnung: Zweck, Art und Umfang der Datenbearbeitung, Einschätzung der möglichen Risiken für die betroffenen Personen sowie gegenwärtigem Stand der Technik. Diese Aufzählung ist nicht abschliessend; es sind alle massgeblichen Interessen in die Beurteilung einzubeziehen (vgl. BVGE 2012/14 E. 9.1; BVGer A-4232/2015 vom 18.4.2017, in sic! 2017 S. 728 E. 9.2.1; David Rosenthal, a.a.O., Art. 7 N. 3, je zur gleich lautenden Bestimmung von Art. 8 Abs. 2 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz [VDSG; SR 235.11]). Im vorliegenden Fall ist insbesondere aufzuzeigen, welche konkreten Risiken (vgl. dazu auch Art. 4 Abs. 1 DSV; vorne E. 2.6) auf dem Spiel stehen und inwiefern ihnen Rechnung getragen werden kann. Gestützt auf die Risikoanalyse sind die verhältnismässigen Massnahmen zu treffen bzw. ist zu begründen, weshalb auf weitergehende Sicherungselemente verzichtet werden kann (vgl. allgemein auch Christa Stamm-Pfister, in Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Aufl. 2014, Art. 7 DSG N. 9). Es reicht nicht aus, wie die STA bloss auf das «Ermessen» der für die Datenbearbeitung verantwortlichen Behörde zu verweisen und eine Umsetzung der Empfehlungen der Aufsichtsstelle erst bei groben Sicherheitsmängeln bzw. geradezu willkürlicher Anwendung der einschlägigen Vorschriften in Aussicht zu stellen (vgl. angefochtene Verfügung E. 16 und 18). Auch wenn der Verwaltung in diesem Zusammenhang durchaus ein Ermessens- bzw. Gestaltungsspielraum zukommt (vgl. Ivo Schwegler, a.a.O., S. 371 f. N. 127 mit Hinweis auf Vortrag Revision KDSG, S. 15), verkennt die Vorinstanz die Tragweite des Verhältnismässigkeitsgrundsatzes.

4.2 Weiter ist zu beachten, dass sich im Zusammenhang mit der Authentifizierungsmethode anspruchsvolle technische Fragen stellen können; darauf hat die Risikobeurteilung soweit erforderlich einzugehen. Insbesondere ist von Interesse, weshalb 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 (vgl. Art. 14 der Verordnung vom 30. November 2012 über die elektronische Geschäftsverwaltung in der Bundesverwaltung [GEVER-Verordnung; SR 172.010.441]). Der Hinweis der STA, die Vorschriften für nicht-

bernische Verwaltungen seien auf BE-GEVER nicht anwendbar (vgl. angefochtene Verfügung E. 21 ff.), trifft zwar zu, ist aber wenig zielführend. Entsprechende Vorgaben können sich auch aus den allgemeinen datenschutzrechtlichen Regelungen und Grundsätzen ergeben, namentlich demjenigen der Datensicherheit. Wie es sich damit im Einzelnen verhält, wird die FIN näher zu prüfen haben.

5.

Am vorliegenden Verfahren sind ausschliesslich kantonale Behörden beteiligt. Es sind daher keine Verfahrenskosten zu erheben (Art. 108 Abs. 2 i.V.m. Art. 2 Abs. 1 Bst. a VRPG). Ersatzfähige Parteikosten sind nicht angefallen.

Demnach entscheidet das Verwaltungsgericht:

1. Auf die Beschwerde wird nicht eingetreten.

2. Es werden weder Verfahrenskosten erhoben noch Parteikosten gesprochen.

3. Zu eröffnen:
   - der Beschwerdeführerin
   - der Staatskanzlei der Kantons Bern

   und mitzuteilen:
   - der Finanzdirektion des Kantons Bern

Der Abteilungspräsident: Der Gerichtsschreiber:

Rechtsmittelbelehrung

Gegen dieses Urteil kann innert 30 Tagen seit Zustellung der schriftlichen Begründung beim Bundesgericht, 1000 Lausanne 14, Beschwerde in öffentlich-rechtlichen Angelegenheiten gemäss Art. 39 ff., 82 ff. und 90 ff. des Bundesgesetzes vom 17. Juni 2005 über das Bundesgericht (BGG; SR 173.110) geführt werden.