AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

TÄTIGKEITSBERICHT 2016

2017/040-09

AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragte:	Ursula Stucki
Stv. Datenschutzbeauftragter:	Tobias Schnelli
Akademische Mitarbeitende:	Priscilla Dipner-Gerber
	Thomas Held
	Carsten Beck
Büro:	Rathausstrasse 45/4
	4410 Liestal
Telefon:	061 552 64 30
Telefax:	061 552 64 31
E-Mail:	datenschutz@bl.ch
Internet:	www.bl.ch/datenschutz

Gestützt auf § 47 Informations- und Datenschutzgesetz (IDG) erstattet die Datenschutzbeauftragte dem Landrat Bericht über ihre Tätigkeit sowie über wichtige Feststellungen und Beurteilungen.

Gestaltung/Illustration: Neeser & Müller, Basel
Druck: Dürrenberger AG, Arlesheim

INHALTSVERZEICHNIS

I. DAS JAHR 2016

Die ASD ist eine formell unabhängige Behörde, die administrativ der Landeskanzlei zugeordnet ist. Sie befasst sich mit den Bereichen Datenschutz und Öffentlichkeitsprinzip.

I.I. DER AUFTRAG DER AUFSICHTSSTELLE DATENSCHUTZ (ASD)

Die ASD hat gemäss § 40 IDG folgenden gesetzlichen Auftrag. Sie

a. kontrolliert nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen;
b. kontrolliert gemäss § 12 vorab Bearbeitungen von Personendaten;
c. berät die öffentlichen Organe in Fragen des Umgangs mit Informationen;
d. berät die betroffenen Personen über ihre Rechte;
e. vermittelt zwischen betroffenen Personen und öffentlichen Organen;
f. nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind.

Im Weiteren ist sie verpflichtet, im Interesse der betroffenen Personen den Erlass von Aufforderungen, Empfehlungen und Weisungen zu prüfen und falls nötig entsprechende Massnahmen einzuleiten, damit ein Datenmissbrauch möglichst verhindert werden kann. Zudem ist die ASD berechtigt und verpflichtet, mit Organen im In- und Ausland zusammenzuarbeiten, welche die gleichen Aufgaben erfüllen (§§ 42 – 45 IDG).

I.II. DAS WESENTLICHE IN KÜRZE

2016 eröffnete die ASD 353 Dossiers. 147 Dossiers betrafen Anfragen von Behörden, wobei sich 11 Anfragen auf das Öffentlichkeitsprinzip bezogen. Zudem wandten sich 69 Privatpersonen Hilfe suchend an die ASD, da sie Fragen zur behördlichen Bearbeitung ihrer Daten hatten. Es wurden ferner 2 Kontrollen abgeschlossen, 13 Vorabkontrollen durchgeführt sowie 59 Eingaben zu unterschiedlichsten Themen geprüft und teils in Stellungnahmen fachlich kommentiert. Im Weiteren wurden die Webseite und einige ältere Merkblätter der ASD überarbeitet, 3 Schulungen durchgeführt, der Tätigkeitsbericht 2015 verfasst und 11 Medienanfragen beantwortet.

Die ASD konnte die Pflicht zur Vorabkontrolle innerhalb der Verwaltung weiter bekannt machen. Dadurch wurden mehr Projekte zur Vorabkontrolle eingereicht, und die ASD konnte einfacher mit den Verantwortlichen in Kontakt treten. Auf diese Weise wurden grössere und kleinere Mängel in Projekten schneller erkannt, was ein rechtzeitiges Reagieren ermöglichte. Auf einzelne Vorabkontrollen musste die ASD aufgrund der prekären Ressourcensituation allerdings verzichten. Trotz der grundsätzlich guten Entwicklung gab es nach wie vor Projektleitende, die wiederholt zu spät zur Beratung kamen oder den Schritt der Vorabkontrolle ganz ausliessen. Zuweilen fehlte gar die gesetzliche Legitimation des Projekts. In solchen Fällen forderte die ASD Nachbesserungen und führte in einem Fall eine anlassbezogene Kontrolle durch. Aus Zeitgründen blieb der ASD oft nichts anderes übrig, als Projekte ungeprüft laufen zu lassen und die Datenbearbeiter an ihre Verantwortung zu erinnern.

Die Digitalisierung der Verwaltung schritt auch im Berichtsjahr weiter voran. Da die Mittel der ASD durch eine parlamentarische Budgetkürzung von 22% zu knapp wurden, kam sie wiederholt an ihre Leistungsgrenzen. Als dann auch noch ein langjähriger und bestens qualifizierter Mitarbeiter die ASD verliess und auch die Datenschutzbeauftragte unplanmässig ausfiel, war an einen adäquaten und zeitgemässen Datenschutz gar nicht mehr zu denken. Dank des überdurchschnittlichen Einsatzes des Datenschutzteams wurde die prekäre Situation nicht publik. Für proaktive Arbeiten blieb aber einmal mehr keine Zeit. Im zweiten Halbjahr besserte sich die Situation ein wenig, die ASD konnte ihren Auftrag im Interesse der Betroffenen trotzdem nur noch unzureichend erfüllen. Die ASD wurde durch die Budgetkürzung finanziell in das Jahr 2011 zurückversetzt und

war somit 2016 bezüglich ihrer Ressourcen stark defizitär ausgestattet. Es zeigte sich in aller Deutlichkeit, dass eine Datenschutzaufsicht nur dann unabhängig, effizient und erfolgreich arbeiten kann, wenn ihr vom Parlament ausreichende Personal- und Sachmittel zur Verfügung gestellt werden.

II. AUSGEWÄHLTE THEMEN 2016

II.I. ZURÜCK AUF FELD EINS

In den letzten zwei Jahren konnte das notwendige IT-Know-how ausgebaut und mit einer Auditorin (CISA) ergänzt werden. Die ASD wurde reorganisiert und konnte ganzheitliche Vorabkontrollen durchführen und in deren Rahmen präventiv Behörden unterstützen und beraten. Im Vergleich zum Vorjahr liefen Projekte vermehrt nach der Methode Hermes ab, und Schutzbedarfsanalysen, Rechtsgrundlagenanalysen sowie Informationssicherheits- und Datenschutz-Konzepte wurden zunehmend zur Vorabkontrolle eingereicht. Im Dezember 2015 entschied das Parlament, dass der ASD 22% ihrer Mittel gekürzt werden sollten, was eine Reduktion von rund 200 000 Franken bedeutete.[1] Die ASD hatte ab Januar 2016 weniger Mittel zur Verfügung als im Jahr 2011 und fiel sprichwörtlich zurück auf Feld Eins.

1 | Zum Vergleich: Budget Datenschutz 2016 Fr. 708 000 – IT-Budget 2016 Fr. 28 Mio.

Es war und ist unbestritten, dass die Finanzlage des Kantons Sparmassnahmen nötig macht, und die ASD war sich auch bewusst, dass auch sie einen Beitrag dazu leisten müsse. Allerdings konnte sie sachlich kaum nachvollziehen, weshalb bei der Kontrollbehörde, die letztlich darauf schaut, dass die gesetzlichen Vorgaben des Souveräns und des Parlaments erfüllt und die Grundrechte vom Staat beachtet werden, die Mittel stark gekürzt wurden, während die Verwaltung mehrheitlich mit weniger drastischen Einsparungen rechnen musste und zudem einen planerischen Vorlauf von rund einem Jahr zugestanden bekommen hatte. Mit der ASD wurde hingegen zu keinem Zeitpunkt über ihre Aufgaben oder Feststellungen gesprochen, und die Tatsache, dass die Kontrollbehörde auch für die Gemeinden und private Institutionen mit Leistungsauftrag (Spitäler, Alters- und Pflegeheime, Spitex etc.) zuständig ist, wurde nicht berücksichtigt. Die Kürzung wurde vom Parlament praktisch diskussionslos beschlossen. Im Resultat hat der Kanton Basel-Landschaft seit Januar 2016 formell eine Datenschutzbehörde, die über Fachwissen in nationalem und internationalem Recht, IT-Sicherheit, IT-Audit etc. verfügt. Es fehlen ihr jedoch die Mittel, um dieses Wissen im erforderlichen Mass gewinnbringend einsetzen zu können. Dies in einer Zeit, in der die Digitalisierung in der Verwaltung, in Spitälern, in Schulen etc. stetig zunimmt, im Kanton zahlreiche ressourcenintensive E-Projekte lanciert werden, das Datenschutzrecht revidiert werden muss und Themen der digitalen Gesellschaft aktueller sind denn je.

Der politische Entscheid gegen einen wirksamen Datenschutz war gefallen, und es galt den Parlamentsentscheid ohne planerischen Vorlauf umzusetzen. Um die Budgetvorgaben einhalten zu können, wurde als erstes auf die Ausbildung von Volontären verzichtet. Im Weiteren verwies die ASD kantonale Dienststellen, die um Rat ersuchten, wiederholt an die Rechtsdienste ihrer Direktionen und stand grundsätzlich nur noch diesen zur Verfügung. Zudem wurden gewisse Stellungnahmen gar nicht mehr verfasst, und Aktivitäten zur Sensibilisierung mussten auf ein absolutes Minimum reduziert werden. Ohne Stellenabbau konnte die Budgetvorgabe des Parlaments aber trotzdem nicht erfüllt werden. Nachdem ein langjähriger, erfahrener und bestens qualifizierter Mitarbeiter den Kanton im Berichtsjahr verlassen hatte, konnte die vakante Stelle aufgrund der reduzierten Mittel nur noch teilweise wiederbesetzt werden. Das abgeflossene Know-how wirkte sich erwartungsgemäss negativ auf die Erledigungseffizienz aus und führte letztlich zu längeren Wartezeiten. Schliesslich fiel auch noch die Datenschutzbeauftragte unerwartet aus und konnte ihre Aufgaben nur noch teilweise wahrnehmen. Trotz eines überdurchschnittlichen Einsatzes des Teams konnten die Anforderungen an einen zeitgemässen Datenschutz nicht mehr erfüllt werden.

Die Digitale Gesellschaft bringt viele Chancen. Sie ist aber auch nicht risikofrei. Damit der Mensch und seine Freiheitsrechte am Ende dieser Entwicklung nicht

auf der Strecke bleiben, braucht es die Auseinandersetzung mit der gesellschaftlichen Bedeutung der gegenwärtigen digitalen Entwicklungen. Und es braucht zudem handlungsfähige Kontrollbehörden, die gegenüber dem Staat reagieren können, wenn es zu rechtsstaatlichen Fehlentwicklungen kommt. Letzteres war 2016 im Kanton nicht mehr gewährleistet.

II.II. DIGITALER PFLICHTKONSUM DER BÜRGERINNEN UND BÜRGER

In der öffentlichen Verwaltung bietet die Digitalisierung eine Chance zur Steigerung der Effektivität, Effizienz und Bürgernähe. Aber anders als in der Wirtschaft haben Bürgerinnen und Bürger bei den Behörden Pflichtkonsum und können nicht einfach den Anbieter wechseln, wenn ihnen der Service nicht vertrauenswürdig erscheint. Die Behörden haben deshalb bei der Nutzung innovativer Informatiklösungen u.a. für die Wahrung der Privatsphäre der Bürgerinnen und Bürger zu sorgen und diesen Aspekt in die Lösungsfindung einzubeziehen. Zudem müssen sie im Rahmen ihrer Projekte an die Betroffenenrechte (Einsichtsrecht, Berichtigungsrecht, Löschung etc.) denken und entsprechende Massnahmen ergreifen.

Auch im Berichtsjahr sahen wir wieder Projekte, bei denen die Frage nach den rechtlichen Grundlagen vernachlässigt wurde. Die Gründe dafür waren vielfältig. So verglichen Involvierte den Staat mit einem privatrechtlich organisierten Unternehmen und kannten das Legalitätsprinzip nicht oder fanden es störend. Andere stellten gar die Frage, ob sich der Kanton die Einhaltung der Gesetze überhaupt noch leisten könne. Man müsse auch diesbezüglich eine Kosten-Nutzen-Analyse durchführen. Die ernsthaft geäusserte Idee, Gesetze nur noch einzuhalten, wenn es sich rechnet, war selbst für die ASD – die viel gewohnt ist – ein neues und sehr irritierendes Argument. Das Team der ASD wurde deshalb auch im Berichtsjahr nicht müde, immer wieder auf das Legalitätsprinzip hinzuweisen und Grundprinzipien des Rechtsstaats zu erklären.

II.III. CLOUD-LÖSUNGEN (K)EIN WUNDERMITTEL?

Cloud-Dienste haben den Vorteil, dass sie oft innerhalb kürzester Zeit bereitgestellt und in Betrieb genommen werden können. Dies verleitet dazu, auf diese Technologie umzusteigen, ohne die erforderlichen Rechtsgrundlagen- und Risikoanalysen durchzuführen. Im Berichtsjahr stellten wir fest, dass oft nicht oder nur oberflächlich geprüft wurde, ob bzw. unter welchen Bedingungen die geplante Datenbearbeitung in der Cloud zulässig wäre. Anfragen und Projekte, welche die eine oder andere Form von Cloud-Computing tangierten, gelangten zudem oft zu spät, d.h. erst kurz vor der Inbetriebnahme, zur ASD.

Die ASD legte bei ihrer Beratung bzw. Vorabkontrolle von Cloud-Lösungen den Fokus auf die spezifischen Cloud-Risiken wie z.B. unzureichende Datentrennung, unverhältnismässige Aufbewahrungsdauer, Kontrollverlust, Zugriff von ausländischen Behörden und generell fehlende Transparenz der Datenbearbeitung. Ein unabdingbarer Baustein bei der Personendatenbearbeitung in der Cloud ist deshalb eine Risikoanalyse sowie die Konzeption und Umsetzung der daraus abgeleiteten Sicherheitsmassnahmen. Dazu gehören auch rechtliche Massnahmen wie die vertragliche Absicherung gegenüber dem Cloud-Anbieter, welche u.a. den Gerichtsstand, den Ort der physischen Speicherung, Verschlüsselungsmechanismen, Subunternehmen sowie Weisungs- und Kontrollbefugnisse regeln muss. Technisch schwierig aber nicht unmöglich ist die Umsetzung der Forderung der Datenschützer, dass bei streng vertraulichen Personendaten das Schlüsselmanagement beim verantwortlichen Organ bleiben muss, da nur so die den Daten angemessene Vertraulichkeit garantiert werden kann. Auffällig war, dass sich Behörden bei wichtigen konzeptionellen Fragen und vertraglichen Regelungen oft gänzlich auf den Cloud-Anbieter verlassen wollten. Dabei wurde ausser Acht gelassen, dass auch bei der Auftragsdatenbearbeitung gemäss § 7 IDG das öffentliche Organ für die Datenbearbeitung verantwortlich bleibt und folglich für die Einhaltung der datenschutzrechtlichen Vorschriften sorgen muss. Der Wunsch der Behörden, Konzeptionelles und Vertragliches möglichst an ein IT-Unternehmen zu delegieren, entstand wohl aufgrund des Ressourcendrucks bei den Verantwortlichen sowie der rechtlichen und technischen Komplexität

von Cloud-Lösungen. Die ASD würde es deshalb begrüssen, wenn die Verantwortlichen in ihren Direktionen mehr Unterstützung finden würden und der Kanton Musterverträge erarbeiten liesse. Die entsprechenden Merkblätter der ASD zur Auftragsdatenbearbeitung und zum Cloud-Computing[2] können dazu als Leitlinie genutzt werden.

2] abrufbar unter https://www.baselland.ch/politik-und-behorden/besondere-behorden/datenschutz/publikationen/merkblatter-muster-schreiben

II.IV. INTERNATIONALES

II.IV.a Entwicklungen im Datenschutzrecht und ihre Auswirkungen auf den Kanton Basel-Landschaft

«No man is an island» – «Kein Mensch ist eine Insel». Diese berühmten Worte des englischen Dichters John Donne treffen in übertragener Weise auch auf das schweizerische und kantonale Datenschutzrecht zu. Bereits heute tauscht der Kanton mit ausländischen Behörden regelmässig Daten aus (Daten betr. Strafverfolgung und Polizei, Gesundheit, Steuern oder Migration etc.), und es ist davon auszugehen, dass die grenzüberschreitende Zusammenarbeit und damit der Austausch von Daten noch zunehmen werden. Europäische Länder dürfen ihre Daten jedoch nur dann in Länder, die nicht Mitglied der EU sind («Drittländer»), weitergeben, wenn das jeweilige Drittland ein angemessenes Schutzniveau gewährleistet. Will der Kanton also mit anderen Ländern weiterhin einen Datenaustausch pflegen, so wird er gewisse internationale Vorgaben einhalten müssen.

Die wichtigsten Neuerungen im Berichtsjahr betrafen die bereits im letzten Tätigkeitsbericht angekündigten gesetzgeberischen Tätigkeiten der EU. Mitte 2016 wurde das lang und intensiv verhandelte europäische Datenschutzpaket offiziell in Kraft gesetzt. Es besteht aus zwei Teilen: Aus der für die Mitgliedstaaten direkt anwendbaren Datenschutz-Grundverordnung (DSGVO)[3] sowie aus der Richtlinie 2016/680 für die Datenbearbeitung im Bereich der Strafverfolgung[4]. Vor allem der zweite Erlass hatte für den Bund und die Kantone unmittelbare Folgen, da die Richtlinie Teil des sogenannten Schengen-Besitzstandes ist. Die Schweiz hatte nur zwei Möglichkeiten: sich zu verpflichten, die Richtlinie ins nationale Recht zu überführen, oder die Kündigung der Schengen-Verträge zu riskieren und u.a. die internationale polizeiliche Zusammenarbeit zu schwächen. Erwartungsgemäss hat sich der Bund für die erste Variante entschieden. Die Richtlinie sieht die Überführung der Bestimmungen ins nationale Recht innert zwei Jahren vor. Diese Frist wurde durch eine Note der EU vom 1. August 2016 ausgelöst. Damit herrscht ein gewisser Zeitdruck für die Gesetzgeber in Bund und Kantonen.

3] http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679

4] http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1491978158208&uri=CELEX%3A32016L0680

Die Ausgangslage bei der Datenschutzgrundverordnung ist etwas anders, da diese für die Schweiz nicht direkt gelten wird. Da allerdings der Austausch von Personendaten mit und innerhalb von EU-Staaten gerade für die schweizerische Wirtschaft eine überragende Bedeutung hat, ist der Schweiz viel daran gelegen, das Niveau auf diesem Gebiet jenem der EU anzugleichen. Denn es wird die EU-Kommission sein, die über den sogenannten Adäquanz-Beschluss darüber entscheidet, ob die schweizerischen Behörden und Unternehmen weiterhin «barrierefrei» Daten fliessen lassen können. Zudem ist davon auszugehen, dass Datenbearbeiter, die Produkte innerhalb der EU anbieten, die DSGVO direkt anwenden müssen.

Der dritte Erlass, welcher die Schweiz direkt betrifft, ist die Modernisierung der Europarats-Konvention 108, deren (wohl) endgültige Fassung im September 2016 publiziert wurde, die aber noch nicht in Kraft getreten ist.[5] Die Schweiz wird jedoch nach aller Voraussicht die neue Konvention ratifizieren und sich damit verpflichten, die dort enthaltenen Bestimmungen ins nationale Recht zu überführen. Bei der Ausarbeitung der Konvention wurde darauf geachtet, dass keine grossen Diskrepanzen zum europäischen Datenschutzpaket entstehen.

5] https://www.coe.int/en/web/data-protection/modernisation-convention108

Natürlich trafen diese drei Erlasse – angesichts der sehr langen Verhandlungsdauer – die Schweiz nicht aus heiterem Himmel. So schickte der Bund bereits gegen Ende 2016 das revidierte Datenschutzgesetz in die Vernehmlassung. Es war abzusehen, dass die politische Diskussion lebhaft ausfallen würde, da insbesondere die Unternehmen einen höheren Aufwand bei der Datenbewirtschaftung befürchten. Dies nicht ganz zu Unrecht, denn eine der Stossrichtungen der Weiterentwicklung des europäischen Datenschutzrechts sind deutlich

weitergehende Informationspflichten. Ebenfalls für eine lebhafte Kontroverse sorgen wird die im Entwurf vorgesehene deutliche Verschärfung der Strafbestimmungen. Auf weitere inhaltliche Details wurde bereits im letztjährigen Tätigkeitsbericht hingewiesen.

Auch die Kantone begannen im Berichtsjahr, sich mit den Grundlagen für die Revisionen der kantonalen Datenschutzgesetze auseinanderzusetzen. Die ASD war dabei in zwei Arbeitsgruppen vertreten, deren Produkt ein durch die Konferenz der Kantonsregierungen zuhanden der Kantone übermittelter Leitfaden zur Anpassung der Datenschutzgesetze bildete. Im innerschweizerischen Vergleich ist der Kanton Basel-Landschaft aufgrund der Tatsache, dass er über ein relativ modernes und junges Informations- und Datenschutzgesetz verfügt, in einer günstigen rechtlichen Situation. Gewisse Anpassungen werden zweifellos nötig sein, aber das Rad wird wohl nicht noch einmal neu erfunden werden müssen. Die ASD wird ihr Know-how für die Anpassungsarbeiten der federführenden Direktion soweit als möglich zur Verfügung stellen.

II.IV.b Urteil betr. die verdeckte Überwachung eines Versicherten durch einen Privatdetektiv

Nicht nur gesetzgeberische Aktivitäten nehmen einen Einfluss auf das schweizerische Recht. Auch im Ausland gefällte Urteile können dies tun, besonders, wenn die Schweiz betroffen ist. Aus einer auch im Jahr 2016 reichhaltigen Rechtsprechung sticht vor allem der Entscheid 61838/10 des Europäischen Gerichtshofes für Menschenrechte (EGMR)[6] in Strassburg heraus. Darin wurde entschieden, dass die verdeckte Überwachung einer Person im öffentlichen Raum durch einen Privatdetektiv einen Verstoss gegen Art. 8 der Europäischen Menschenrechtskonvention EMRK, das Recht auf Achtung des Privat- und Familienlebens, darstelle. Gerügt wurde insbesondere, dass die entsprechenden Bestimmungen im allgemeinen Teil des Sozialversicherungsgesetzes sowie im Unfallversicherungsgesetz zu unbestimmt seien. Damit sei die Vorhersehbarkeit einer solchen Überwachung nicht gegeben, und wichtige «Nebenpunkte» wie die Überprüfung, Anordnung, Aufbewahrungsdauer und Löschung der Daten seien nicht geregelt. Auch verwarf der EGMR die Ansicht des Bundesgerichtes, dass eine solche Überwachung dann kein schwerer Eingriff in die Privatsphäre sei, wenn sie nur auf öffentlichem Grund erfolge.

6] http://hudoc.echr.coe.int/eng#{«itemid»:[«001-167490»]} auf Englisch

Dieser viel beachtete Entscheid löste bereits auf Bundesebene gesetzgeberische Aktivitäten aus. Da der Sozialversicherungsbereich bundesrechtlich geregelt ist, stellte sich für die Kantone in diesem Zusammenhang einzig die Frage, ob allfällig vorhandene Normen der Überwachung im Sozialhilfebereich präziser formuliert werden müssen.

Ein Eingriff in die Grundrechte hat immer aufgrund einer gesetzlichen Grundlage zu erfolgen. Je schwerer der Eingriff in das Grundrecht ist, desto präziser muss diese gesetzliche Grundlage ausgestaltet werden. Selbstverständlich gibt es vor allem im Bereich der Sicherheit Sachverhalte, die in so vielfältiger Weise auftreten können, dass man sie nur mit relativ offenen Begriffen im Gesetz formulieren kann. Umso wichtiger ist es aber in diesen Fällen, dass die «flankierenden» Bestimmungen, eben jene zum Verfahren der Datenbearbeitung, so präzise ausfallen, dass die Gefahr des Missbrauchs der bearbeiteten Daten minimiert wird und die betroffenen Personen ihre Rechte wahrnehmen können. Die ASD hat in den letzten Jahren wiederholt in Mitberichten und Vernehmlassungen auf diese Tatsache aufmerksam gemacht. Präzise gesetzliche Grundlagen sind überdies nicht nur von Verfassung, Lehre und Rechtsprechung gefordert, sondern sie helfen auch, langwierige und kostenintensive Verfahren zu verhindern. Im Fall, der nun vom EGMR entschieden wurde, lag die Überwachung zehn Jahre zurück.

III. AUS DEM BERATUNGS-ALLTAG

Im Folgenden werden ein paar Fälle aus der juristischen und technischen Beratung dargestellt, die sich in Aufwand und Komplexität unterscheiden.

III.I. FOTOAUFNAHMEN VON SCHÜLERINNEN UND SCHÜLERN DURCH DIE SCHULLEITUNG

Die Eltern eines elfjährigen Kindes wurden bei der ASD vorstellig, weil sie nicht damit einverstanden waren, dass die Schulleitung anlässlich einer Visite einer Schulstunde zum Zwecke der Beurteilung einer Lehrperson Fotoaufnahmen ihres Kindes machte und diese in das Personaldossier der beurteilten Lehrperson ablegte. Die Eltern bemängelten insbesondere, dass der genaue Zweck der Fotoaufnahmen vorab nicht erklärt worden und die Einwilligung zu den Fotoaufnahmen nicht über die Eltern erfolgt sei.

Die ASD zeigte den Eltern auf, dass die Einwilligung bezüglich Fotoaufnahmen bei einem elfjährigen Kind grundsätzlich bei den Erziehungsberechtigten und nicht beim Kind selbst eingeholt werden sollte, da die Urteilsfähigkeit in diesem Alter noch nicht gegeben ist. Zudem wies die ASD darauf hin, dass entsprechende Fotos zur Aufgabenerfüllung der Schulleitung bzw. zur Beurteilung einer Lehrperson grundsätzlich nicht notwendig seien. Schliesslich konnte die ASD die Eltern auch darüber informieren, dass bei entsprechenden Fotoaufnahmen, losgelöst von der datenschutzrechtlichen Problematik, auch das Recht am eigenen Bild gemäss dem schweizerischen Zivilgesetzbuch (ZGB) tangiert werde.

Die ASD suchte anschliessend das Gespräch mit der Schulleitung und konnte dieser anlässlich einer gemeinsamen Besprechung die gegenüber den Eltern gemachten Ausführungen und Überlegungen darlegen. Die Schulleitung erklärte gegenüber der ASD, bei künftigen Fotoaufnahmen die datenschutzrechtlichen Vorgaben zu erfüllen.

III.II. HINWEIS AUF EINEN STRAFBEFEHL AN DAS KANTONSSPITAL BL ALS ARBEITGEBER DURCH DAS AMT FÜR MIGRATION

Dem Amt für Migration lag ein Strafbefehl gegen eine ausländische Person wegen Fahren in angetrunkenem Zustand vor. Die betroffene Person arbeitete als Pflegefachkraft beim Kantonsspital Baselland. Das Amt für Migration wollte nun von der ASD wissen, ob es dem Kantonsspital Baselland eine Mitteilung über das Vorliegen des Strafbefehls machen dürfe.

Eine Datenbekanntgabe kann gemäss IDG immer dann erfolgen, wenn entweder eine gesetzliche Grundlage hierfür besteht oder die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder aber im Einzelfall jeweils eine Einwilligung vorliegt. Mangels Vorliegen einer dieser Voraussetzungen konnte die ASD dem Amt für Migration mitteilen, dass eine Mitteilung des Vorliegens eines Strafbefehls an das Kantonsspital Baselland ohne Einwilligung der betroffenen Person nicht möglich sei. Ob allenfalls die betroffene Person zu einer Mitteilung verpflichtet ist, richtet sich nach den anwendbaren arbeitsrechtlichen Bestimmungen.

III.III. DURCHBRECHUNG EINER DATENSPERRUNG UND GEWÄHRUNG DES RECHTLICHEN GEHÖRS

Eine Gemeinde gelangte an die ASD und wollte wissen, ob sie eine Person, welche ihre im Einwohnerregister eingetragenen Daten hat sperren lassen, anhören und damit das rechtliche Gehör gewähren muss, auch wenn aufgrund des Sachverhalts klar ist, dass die Voraussetzungen für eine Durchbrechung der Sperre im Sinne von § 26 IDG erfüllt sind. Konkret ging es um ein Inkassobüro, das die Adresse der im Einwohnerregister verzeichneten Person benötigt hatte. Das Inkassobüro hatte im Auftrag einer anderen Gemeinde mittels Verlustschein ausstehende Steuerschulden eingetrieben.

Mit der Gewährung des rechtlichen Gehörs, einem in unserem Rechtsstaat fest verankerten Rechtsgrundsatz, soll sichergestellt werden, dass eine Behörde

die betroffene Seite anhört bzw. sich die betroffene Person ebenfalls zu einem Sachverhalt äussern kann, bevor die Behörde einen Entscheid fällt und eine Verfügung erlässt. Die ASD empfahl deshalb der anfragenden Gemeinde, die Person, welche ihre Daten hat sperren lassen, zum Sachverhalt zu befragen, damit diese allfällige berechtigte Einwände, welche gegen eine Bekanntgabe ihrer Daten sprechen, geltend machen könne. Gewährt die Gemeinde also das rechtliche Gehör, macht sie verfahrensrechtlich alles korrekt und steht letztlich auf der sicheren Seite.

III.IV. FALSCHE ZUSTELLUNG EINES ZAHLUNGSBEFEHLS DURCH DIE POST

Einer Person wurde durch die Post fälschlicherweise ein Zahlungsbefehl einer benachbarten Person in den Briefkasten gelegt. Die anfragende Person war sich bewusst, dass der Post hier ein Fehler unterlaufen war. Sie war jedoch erstaunt über die Tatsache, dass ein Zahlungsbefehl durch das Betreibungsamt offen, ohne Couvert, verschickt worden war und wollte daher von der ASD wissen, ob dies aus datenschutzrechtlicher Sicht zulässig sei.

Die ASD konnte der Person mitteilen, dass die Zustellung gemäss dem Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) offen erfolgt. Der Zahlungsbefehl wird vom Betreibungsamt doppelt ausgefertigt. Bei der Übergabe durch die Post muss der Postbote auf beiden Ausfertigungen bescheinigen, an welchem Tag und an wen die Zustellung erfolgt ist (vgl. Art. 72 SchKG). Falls der Postbote den Zahlungsbefehl offen in einen falschen Briefkasten legt, haftet er bzw. die Post für die nicht korrekte Zustellung. Zudem untersteht der Postbote dem Amts- und Postgeheimnis, welches durch die nicht korrekte Zustellung verletzt wird und grundsätzlich strafrechtlich verfolgt werden könnte.

III.V. ZUSTELLUNG EINER VERANLAGUNGSVERFÜGUNG AN EINE UNFALLVERSICHERUNG ZWECKS ABKLÄRUNG DER MÖGLICHKEIT DES RÜCKGRIFFS AUF EINEN UNFALLVERURSACHER

Eine Gemeinde wurde bei der ASD vorstellig, weil sie wissen wollte, ob sie einer Unfallversicherung eine aktuelle Veranlagungsverfügung einer in der Gemeinde wohnhaften Person, welche einen Unfall verursacht hatte, aushändigen darf. Die Versicherung machte geltend, dass sie diese Angaben für die Abklärung benötige, ob ein Rückgriff auf die in der Gemeinde wohnhafte haftpflichtige Person möglich sei, und stützte sich dabei auf Art. 32 des Allgemeinen Teils des Sozialversicherungsrechts (ATSG).

Die ASD konnte der Gemeinde mitteilen, dass die Versicherung zwar als ein Organ der Sozialversicherung gemäss Art. 32 ATSG anzusehen sei. Damit jedoch Auskünfte erteilt werden könnten, müssten diese für den Rückgriff auf den haftpflichtigen Dritten tatsächlich erforderlich sein (Art. 32 Abs. 1 ATSG). Gemäss Schreiben der Versicherung war der Kausalzusammenhang zwischen dem schädigenden Ereignis und dem Schaden gegeben. Der Unfallverursacher war damit für den zugefügten Schaden haftbar. Folglich hätte die Versicherung, unabhängig von der Leistungsfähigkeit des Unfallverursachers bzw. des haftpflichtigen Dritten, Rückgriff auf diesen nehmen können. Angaben über die Vermögensverhältnisse des Unfallverursachers bzw. des haftpflichtigen Dritten waren also für den Regress nicht erforderlich. Die Gemeinde konnte deshalb die Herausgabe der aktuellen Veranlagungsverfügung verweigern.

III.VI. EINSICHT IN ALTE KOMMISSIONSPROTOKOLLE

Die leitende Person einer Gemeindeverwaltung gelangte an die ASD, weil sie sich nicht sicher war, ob und allenfalls wie weit ein neu gewählter Vorsitz einer Gemeindekommission Einblick in alte Kommissionsprotokolle haben darf.

Die ASD konnte der leitenden Person der Gemeindeverwaltung mitteilen, dass der neue Vorsitz der Kommission grundsätzlich in diejenigen Protokolle Einsicht nehmen darf, welche für seine Aufgabenerfüllung erforderlich sind. Das können durchaus auch alte Protokolle sein, insbesondere dann, wenn ein Ge-

schäft noch nicht abgeschlossen worden ist und deshalb bereits Verhandeltes und Besprochenes für die Entscheidungsfindung relevant sind. In Protokolle, die zur Aufgabenerfüllung nicht mehr erforderlich sind, muss folglich keine Einsicht gewährt werden.

III.VII. PUBLIKATION DER NAMEN DER BESCHWERDEFÜHRENDEN DURCH EINE KIRCHGEMEINDE

Mehrere Personen hatten gegen einen Beschluss der Kirchgemeindeversammlung Beschwerde eingelegt. Im Rahmen des Verfahrens ist die Beschwerde dem Präsidium der zuständigen Kirchgemeinde zur Stellungnahme vorgelegt worden. Daraufhin hat das Präsidium der zuständigen Kirchgemeinde die Namen sämtlicher Beschwerdeführenden im Publikationsorgan, auf der Homepage der Kirchgemeinde sowie in einem Anschlagkasten vor der Kirche veröffentlicht. Eine der betroffenen Personen wollte nun von der ASD wissen, wie dieses Vorgehen aus datenschutzrechtlicher Sicht zu beurteilen sei und ob sie sich allenfalls zu Wehr setzen könne.

Mit einer Publikation der Namen sämtlicher Beschwerdeführenden werden Personendaten bekanntgegeben. Eine solche Bekanntgabe ist gemäss IDG immer dann möglich, wenn eine gesetzliche Grundlage dazu verpflichtet oder berechtigt, die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder die betroffene Person im Einzelfall zugestimmt hat. Weil keine gesetzliche Grundlage besteht, die Bekanntgabe der Namen der Beschwerdeführenden auch nicht zur Aufgabenerfüllung der Kirchgemeinde erforderlich ist und keine Einwilligung der Betroffenen vorlag, konnte die ASD der Person mitteilen, dass die Publikation der Namen widerrechtlich gewesen sei. Die ASD konnte die Person zudem auf § 25 IDG aufmerksam machen, wonach sie von der Kirchgemeinde verlangen kann, die Widerrechtlichkeit des Bearbeitens schriftlich festhalten zu lassen.

III.VIII. FÜHRUNG DER KONFESSION ALS MERKMAL IM EINWOHNERREGISTER

Eine Person wandte sich an die ASD, da eine Gemeindeverwaltung ihr gegenüber ausgeführt hatte, dass im Einwohnerregister bei Einwohnerinnen und Einwohnern, welche nicht einer der drei im Kanton anerkannten Landeskirchen angehören, der Vermerk «Unbekannt» bzw. «Andere» eingetragen wird. Die Person wollte wissen, weshalb Mitglieder einer der drei im Kanton anerkannten Landeskirchen aus ihrer Sicht datenschutzmässig schlechter gestellt würden als Mitglieder einer anderen Religion.

Das Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (Registerharmonierungsgesetz, RHG) definiert den minimalen Inhalt der im Einwohnerregister zu führenden Daten zu einzelnen Identifikatoren und Merkmalen einer verzeichneten Person. Gestützt auf das RHG wird vom Bundesamt für Statistik der amtliche Katalog der Merkmale erlassen, in welchem die Merkmale genauer umschrieben und definiert werden. Das kantonale Kirchengesetz und das RHG halten fest, dass die drei anerkannten Landeskirchen im Einwohnerregister zu erfassen sind. Alle übrigen Religionen sind mit dem Code «Unbekannt» oder «Andere» zu registrieren. Die entsprechende Handhabung ist darüber hinaus auch aus (kirchen)steuerrechtlichen Gründen nötig.

III.IX. PUBLIKATION DER WOHNADRESSE DES VERKÄUFERS BEIM VERKAUF EINER LIEGENSCHAFT

Der Verkäufer einer Liegenschaft gelangte an die ASD, weil er nicht wollte, dass aufgrund des Verkaufs sein Wohnort im Amtsblatt publiziert wird. Er wollte durch die ASD abgeklärt haben, wie die Situation aus datenschutzrechtlicher Sicht zu beurteilen ist.

In § 2 Abs. 1 der kantonalen Verordnung über die Veröffentlichung von Eigentumsübertragungen wird festgehalten, dass bei einem Verkauf einer Liegenschaft unter anderem der Name und der Wohnort der veräussernden Person im Amtsblatt veröffentlicht werden. Somit konnte die ASD der anfragenden Person mitteilen, dass für die Publikation die nach IDG erforderliche gesetzliche Grundlage bestehe und die Behörde den Wohnort habe publizieren dürfen.

III.X. ÜBERMITTLUNG VON MEDIZINISCHEN BEFUNDEN AUS DER FAHREIGNUNGS-PRÜFUNG DURCH ÄRZTE AN DIE MFK

Eine 72-jährige Person musste sich der gesetzlich vorgeschriebenen Fahreignungsprüfung durch einen Arzt unterziehen. Der Arzt übermittelte danach seinen Bericht an die im Kanton zuständige Stelle, die Motorfahrzeugkontrolle (MFK). Die betroffene Person zeigte sich besorgt, dass der Befund ihres Arztes an die MFK und nicht an eine polizeiliche Behörde weitergeleitet wurde und befürchtete zudem, dass ihre Unterlagen nicht vertraulich behandelt würden, weshalb sie sich an die ASD wandte.

Nach Abklärung der rechtlichen Situation konnte die ASD der Person mitteilen, dass für die Zustellung des Resultats der Fahreignungsprüfung an die MFK durch den Arzt mit der bundesrechtlichen Verkehrszulassungsverordnung (VZV) eine gesetzliche Grundlage für die Bekanntgabe bestehe. Zudem verwenden die MFK bzw. die Ärzte das korrekte, im Anhang 3 der VZV aufgeführte Formular. Und schliesslich konnte die ASD die Person darauf hinweisen, dass die MFK die Daten nur im gesetzlich zulässigen Rahmen bearbeiten dürfe und dabei insbesondere an das Verhältnismässigkeitsprinzip gebunden sei. Die MFK darf die Daten bearbeiten, soweit dies zur Aufgabenerfüllung tatsächlich erforderlich ist.

III.XI. PERSONENSICHERHEITS-PRÜFUNG

Dem Staat stehen viele Daten zur Verfügung. Erfahrungsgemäss ist die Versuchung gross, diesen Datenpool ohne rechtliche Legitimation zu nutzen und Daten zweckfremd zu bearbeiten. Im Berichtsjahr wurde der ASD von zwei Fällen berichtet, in denen polizeiliche Datenbanken für illegale Personensicherheitsprüfungen abgefragt wurden. Später wurde bekannt, dass auch in weiteren Fällen Personen und deren Lebenspartner ohne gesetzliche Grundlagen sicherheitsüberprüft wurden. Dieses heimliche Abfragen von polizeilichen Datenbanken verletzte nicht nur das Legalitätsprinzip und das Transparenzgebot. Die betroffenen Personen wurden weder vor noch nach der Prüfung über die Abfragen und deren Ergebnisse informiert und konnten dazu folglich auch keine Stellung nehmen.

Die ASD verlangte, dass die illegalen Abfragen gestoppt würden und empfahl, das Thema Personensicherheitsprüfung auf eine gute rechtliche Basis zu stellen. Nachdem das Personalamt in einem ersten Schritt eine Weisung über die im Anstellungsverfahren zu erhebenden Registerauszüge erlassen hatte, übernahm die Sicherheitsdirektion die Leitung des Projekts «Personensicherheitsprüfung». Im Rahmen dieses Projekts müssen die einzelnen Funktionen innerhalb der Verwaltung, die ein Sicherheitsrisiko darstellen könnten, evaluiert werden. In einem nächsten Schritt müssen Risikostufen definiert und den einzelnen Funktionen zugewiesen werden. So sind die Funktionen Generalsekretär, Buchhalter oder IT-Administrator wohl mit höheren Risiken verbunden als beispielsweise Lehrer. Die Definition der Funktionen und die Zuteilung der Risikostufen auf die Funktionen bedeutet viel Arbeit. Will man jedoch eine professionelle und rechtmässige Personenprüfung einführen, so führt kein Weg an diesem Aufwand vorbei. Erst wenn die notwendige Projektarbeit geleistet und ein entsprechendes Gesetz erlassen ist, steht einer rechtmässigen Personensicherheitsprüfung nichts mehr im Weg.

III.XII. REVISION DER INFORMATIK- UND PROJEKTMANAGEMENT-VERORDNUNG

Die ASD nahm die Gelegenheit wahr, bereits bei der Erarbeitung der Informatik- und Projektmanagementverordnungen ihren Beitrag zu leisten, und konnte somit ihre Erfahrungen zielführend einbringen. Sie begrüsste die Klärung der Verantwortlichkeiten in der Informatikverordnung zur Sicherstellung der Informationssicherheit auf der Stufe der Dienststellen. Sie erhofft sich, dass dadurch das Bewusstsein der verantwortlichen Organe in ihrer Rolle als Informationseigner gestärkt wird. Auch die durch die Revision der Projektmanagementverordnung verstärkte Governance in Projekten wurde begrüsst, da die ASD bei ihrer Aufsichtstätigkeit immer wieder auf Projektabwicklungen stiess, die methodische

Mängel aufwiesen. Diese Mängel führten u.a. zu Risiken bezüglich der Angemessenheit der Informationssicherheits-Massnahmen. Musste inhaltlich nachgebessert werden, so hörten wir oft, «Der Datenschutz» führe zu Mehraufwand. Die ASD verlangt jedoch keine Projektergebnisse, die in einem geordneten Projekt nicht sowieso erarbeitet werden müssten.

Kritisch beurteilte die Datenschutzbeauftragte die Verordnungsbestimmung, wonach Kleinprojekte ohne die Anwendung einer spezifischen Projektmanagement-Methode abgewickelt werden können. Dies birgt erfahrungsgemäss die Gefahr, dass bei der Bearbeitung von Personendaten oder weiterer vertraulicher Daten die Risiken nicht analysiert und notwendige Massnahmen nicht angemessen konzipiert werden.

III.XIII. PROTOKOLLIERUNG

Im Berichtsjahr wandten sich mehrere öffentliche Organe an die ASD, um sich in Sachen Protokollierung von Datenbearbeitungen beraten zu lassen. Die Fragen betrafen u.a. den Detaillierungsgrad der Protokollierung, die Aufbewahrungsfrist und die Auswertung der Protokolldaten. Sowohl im Datenschutzgesetz als auch in Spezialgesetzen sind Regelungen enthalten, aus denen sich die Pflicht zur Protokollierung entweder direkt ergibt oder aber davon ableiten lässt.

Eine Protokollierung ist oft zur Nachvollziehbarkeit staatlichen Handelns erforderlich. So können beispielsweise die ASD oder andere mit einer Revision befasste Behörden die Rechtmässigkeit von Datenzugriffen nachträglich nur kontrollieren, wenn diese protokolliert wurden. Die Protokolldateien stellen dabei eine neue Datensammlung dar und unterliegen folglich selber wieder den datenschutzrechtlichen Vorgaben. Sind Protokolle zum Zwecke der Revision entstanden, so dürfen sie nicht für andere Zwecke verwendet werden (Zweckbindungsgebot). Aber auch das Arbeitsrecht schränkt die Verwendung von Protokollen ein. So ist es grundsätzlich nicht zulässig, das Verhalten der Mitarbeitenden mithilfe von Protokolldaten systematisch zu kontrollieren. Art, Umfang und Dauer der Protokollierung sind auf das zur Erfüllung des Protokollierungszwecks erforderliche Mass zu beschränken. Die ASD stellte wiederholt fest, dass diese Zusammenhänge nicht bekannt waren und kaum Hilfestellungen für die konkrete Ausgestaltung der Protokollierung existieren. Die ASD wird deshalb 2017 einen Leitfaden als grundlegende Orientierungshilfe publizieren.

IV. VORABKONTROLLE ALS KONTROLL-INSTRUMENT DER COMPLIANCE

Die ASD präsentierte dem kantonalen ITO-Rat die Erfolgsfaktoren einer Vorabkontrolle und konnte aufzeigen, dass nachträgliche Nachbesserungen in der Regel kostenintensiv sind und zu unnötigen Verzögerungen in der Einführungsphase oder im Betrieb führen. Diese Information war wichtig, da Compliance (Regelkonformität) letztlich von der obersten Führungsebene getragen werden muss. Nur wenn sie vom Management getragen wird, kann sie sich im Unternehmen resp. in der Verwaltung entfalten. Die Vorabkontrolle als Kontrollinstrument der Compliance wurde im Berichtsjahr mehr berücksichtigt als noch zu Beginn ihrer Einführung. Die Prüfung, ob ein Projekt für eine Vorabkontrolle relevant ist, ist jedoch noch längst nicht für alle Projektleitenden ein selbstverständlicher Teil des Projekts.

Bisher betrafen sämtliche Vorabkontrollen öffentliche Organe der kantonalen Verwaltung. Im Berichtsjahr waren noch elf Projekte aus dem Vorjahr aktiv in der Vorabkontrolle bzw. in der Abklärung zur Vorabkontrolle. Vierzehn neue Projekte gingen zur Vorabkontrolle ein. Bei sechs Eingaben entschied die Aufsichtsstelle, keine Vorabkontrolle durchzuführen, weil die Vorprüfung auf der Basis der abgegebenen Dokumentation ergab, dass die Datenbearbeitung keine besonderen Risiken für die Rechte und die Freiheit der betroffenen Personen mit sich bringt (§ 12 Abs. 1 IDG). Zu drei Projekten konnte keine Vorabkontrolle durchgeführt werden, weil sie zu spät im Projektablauf eintrafen und datenschutzrechtliche

Empfehlungen im Projekt keine Wirkung mehr hätten entfalten können. Vier Vorabkontrollen konnten im Berichtsjahr abgeschlossen werden. In einzelnen Fällen führte die Delegation wichtiger Projektentscheide vom verantwortlichen Organ zur Projektleitung zur Inbetriebnahme von Lösungen, ohne den erhöhten Risiken mit angemessenen Massnahmen begegnet zu sein und ohne den Abschluss der Vorabkontrolle gemäss § 12 IDG abgewartet zu haben. Bezeichnenderweise waren dies meist IT-gesteuerte Projekte, in denen die Informatik den Takt angab, ohne sich gross über die Konzeption der Datenschutz- und IT-Sicherheitsmassnahmen Gedanken zu machen. Man war zum Teil der Meinung, um den Datenschutz und die Informationssicherheit könne man sich dann nach der Inbetriebnahme kümmern. In Zeiten von Cybercrime kann eine solche Verhaltensweise auch einmal zu grösserem Schaden führen. Und Nachbesserungen im Betrieb sind – wie bereits erwähnt – meist zeitintensiv und teuer.

Schwerpunktmässig zeigte sich auch in diesem Berichtsjahr bei den vorab kontrollierten Vorhaben Handlungsbedarf bei der risikobasierten Konzeption der Sicherheitsmassnahmen, bei Berechtigungskonzepten und Outsourcingverträgen. Oft begegnete die ASD auch Projektbeteiligten, die nicht wussten, dass die Informationseigner für die Einhaltung der datenschutzrechtlichen Vorgaben und die IT-Sicherheit verantwortlich sind (§ 6 IDG). Es gab aber auch Projektleitende, welche die methodischen Vorgaben nicht kannten oder unklare resp. unerfüllbare Projektaufträge erhalten hatten.

In Sachen Informationssicherheit bestand für die Projektmitarbeitenden die Herausforderung, aus dem Schutzbedarf für die Informationen eine authentische Risikoanalyse zu erstellen und daraus angemessene Schutzmassnahmen zu konzipieren. Nicht selten wurden da von der ASD Beratungsleistungen in einer Tiefe erwünscht, die sie aufgrund ihrer Rolle und ihrer Ressourcen nicht leisten konnte. Schwierig gestalteten sich aus diesem Grund die Vorabkontrollen vor allem dann, wenn seitens des öffentlichen Organs Personen Projektrollen übernehmen mussten, für die ihnen das fachliche Know-how fehlte. So erhielt die ASD im Berichtsjahr beispielsweise Rechtsgrundlagenanalysen zur Prüfung, die Projektleitende statt Personen mit juristischer Fachkompetenz erarbeitet hatten, und ISDS-Konzepte, welche nicht durch Sicherheitsbeauftragte erstellt worden waren. In der Folge mussten die Dokumente wiederholt überarbeitet und geprüft werden, was zu einem Mehraufwand im Projekt und bei der ASD führte.

Vorabkontrollen zeigten zudem, dass die implementierten Berechtigungen sich oft nicht an den gesetzlichen Vorgaben und den Aufgaben der Personen orientierten, sondern eher Ad-hoc-Wünschen folgten. Dadurch war es oft schwierig nachvollziehbar, welche Berechtigungen aufgrund welcher Basis einem Benutzer/einer Benutzerin zugeteilt sind. Ein sorgfältig geplantes und in Übereinstimmung mit den gesetzlichen Grundlagen auf die Anforderungen der Geschäftsprozesse abgestimmtes Rollen- und Berechtigungskonzept bildet einen wichtigen Grundstein für eine datenschutzkonforme und nachvollziehbare Datenbearbeitung in den öffentlichen Organen und ist der Garant für die Einhaltung des Amtsgeheimnisses. Die ASD hat deshalb gegen Ende des Berichtsjahres einen Leitfaden entworfen, welcher den verantwortlichen Stellen eine Hilfestellung geben wird, wie sie ihre Berechtigungskonzepte gestalten und umsetzen können. Er wird im ersten Halbjahr 2017 veröffentlicht.

Die ASD erhofft sich durch die Revision der seit Jahren geltenden Projektmanagementverordnung einen neuen Bewusstseins- und Ausbildungsschub, welcher sowohl beim öffentlichen Organ als auch bei den prüfenden Stellen Entlastung bringt. Bei Projekten, in denen die Zentrale Informatik involviert war, wurde durch das von der Leitung ZI vorgegebene strukturierte Projektvorgehen die Qualitätssteigerung teilweise bereits spürbar. Ausserdem war ein Lernprozess einzelner öffentliche Organe zu erkennen, welche bereits eine oder mehrere Vorabkontrollen durchlaufen und den Mehrwert der ISDS-Arbeiten mit frühzeitigem Kontakt zur ASD erkannt haben. Um die Verzahnung der Vorabkontrolle mit der in der kantonalen Verwaltung vorgegebenen Projektmanagementmethode HERMES zu optimieren, wurde im Berichtsjahr eine auf den Erfahrungen basierende Abstimmung der Prozesse begonnen. Als Ziel gilt immer noch, die Qualität der Projekte bzgl. Datenschutz und Informationssicherheit zu erhö-

hen und gleichzeitig den Aufwand der Projektleitenden und der Aufsichtsstelle zu minimieren.

V. KONTROLL-TÄTIGKEITEN

Die Aufsichtsstelle Datenschutz pflegt eine rollende, risikobasierte Kontrollplanung. Da mehr Projekte zur Vorabkontrolle eingereicht wurden, blieben weniger Ressourcen für eigentliche Kontrollen.

Die rollende Planung führt dazu, dass die Planung der Kontrollen und die Durchführung nicht zwingend im selben Jahr stattfinden. Neben anlassfreien Kontrollen wurden auch sogenannte anlassbedingte Kontrollen durchgeführt. Im Berichtsjahr war dies eine, welche aufgrund einer unterlassenen Vorabkontrolle gestartet wurde.

Die Berichte, welche die ASD im Rahmen der Kontrolltätigkeit erstellt oder erstellen lässt, sind samt den ihnen zugrunde liegenden Materialien nicht öffentlich (§ 41 IDG). Dies einerseits deshalb, weil die kontrollierten Organe andernfalls bei Kontrollen der ASD möglicherweise wichtige Informationen vorenthalten würden und die Aufsichtstätigkeit nicht die gewünschte nachhaltige Wirkung erzielen könnte. Ein weiterer Grund liegt darin, dass mit einer Publikation von Schwachstellen das Risiko von deren Ausnutzung durch Angreifende erhöht wird.

V.I. DAS ZENTRALE PERSONENREGISTER ARBO

In den letzten Jahren ist das kantonale Personenregister arbo zu einem Kernelement des kantonalen Personendatenaustauschs geworden. Personendaten aus arbo werden rege abgefragt und ausgetauscht. Den grössten Teil von «arbo» machen die Daten der Einwohnerregister der Gemeinden aus, d.h. die Angaben zu den natürlichen Personen mit Wohnsitz oder Aufenthalt im Kanton Basel-Landschaft. Daneben enthält das kantonale Personenregister bestimmte Angaben zu den natürlichen und juristischen Personen mit Grundeigentum im Kanton Basel-Landschaft. Aus datenschutzrechtlicher Sicht vereint arbo verschiedene Risiken für die im System verzeichneten Personen (Abrufverfahren, besondere Personendaten, Datenbearbeitung durch mehrere öffentliche Organe). Eine datenschutzrechtliche Kontrolle im arbo-Kontext wurde Ende 2015 im Detail geplant. Die Kontrolle vor Ort wurde im Berichtsjahr durchgeführt und mit einem Schlussbericht im Herbst abgeschlossen.

Schwerpunkte dieser datenschutzrechtlichen Kontrolle bildeten die zentralen und dezentralen Verantwortlichkeiten bzgl. Bestätigung der Anschlussvoraussetzungen, Massnahmen Informationssicherheit und Datenschutz, Information Life Cycle, Durchführung von gesetzlich geregelten internen Kontrollen der Zugriffe und die konkreten Schutzmassnahmen. Ausserdem prüfte die ASD – wie bei allen Kontrollen – die Umsetzung weiterer datenschutzrechtlicher Vorgaben zur Verhältnismässigkeit, Aufbewahrung und Löschung von Daten usw.

Dazu wurden im ersten Halbjahr 2016 Kontrollen vor Ort bei dem für den Betrieb von arbo verantwortlichen Organ, bei einem Generalsekretariat und bei zwei dezentralen Datenbezügern durchgeführt. Die Kontrollen ergaben drei Feststellungen zu dringlich zu behebenden Schwachstellen und vierzehn Schwachstellen, welche ein mittleres Risiko bargen. Zwei Feststellungen wurden als Optimierungspotenzial ausgewiesen.

Im Rahmen der Kontrolle fiel positiv auf, wie stark die Fachstelle arbo darauf achtet, die öffentlichen Organe jeweils auf ihre Verantwortung gemäss § 6 IDG hinzuweisen und diese Verantwortung in den Abläufen konsequent zu verankern. Ebenso wurde in arbo selbst streng darauf geachtet, dass die vom Regierungsrat beschlossenen Zugriffsrechte korrekt und aktuell umgesetzt werden. Dies war und ist notwendig, weil das Benutzerverzeichnis nicht mit den Eintritts- und Austrittsprozessen synchronisiert ist.

Dringender Handlungsbedarf wurde namentlich beim Prüfungsablauf der Anschlussverfahren und bei der Abwicklung von arbo-Anschlussprojekten ausgemacht, welche nicht oder nur partiell nach der im Kanton geltenden Projektfüh-

rungsmethode HERMES durchgeführt werden. Dies schlug sich teilweise auch in ungenügenden Analysen der Rechtsgrundlagen für den Datenbezug nieder. Zudem wurden die Vorgaben für abfragende Stellen oft nicht berücksichtigt, und Informationssicherheits- und Datenschutzkonzepte waren oft unzureichend. Dies war fallweise auch auf eine fehlerhafte Beratung durch Verantwortliche zurückzuführen, welche suggerierte, die Umsetzung gesetzlicher Vorgaben liesse sich einer Kosten-Nutzen-Analyse unterziehen, und es bestehe die Möglichkeit, auf eine rechtmässige Umsetzung zu verzichten. Die Umsetzung von § 23 Abs. 2 ARV, wonach die abfragende Stelle intern kontrollieren muss, ob die Abfragen rechtmässig erfolgen, fand im Berichtsjahr kaum statt. Die ASD fand im Rahmen ihrer Kontrolle zwei Bereiche, welche mehr Daten bearbeiteten als nötig.

Einzelne Schwachstellen wurden ausserdem bei der Umsetzung der Informationssicherheitsrichtlinien festgestellt. Dabei fiel auf, dass die Kommunikation von neuen oder angepassten Richtlinien innerhalb der Direktion und ausserhalb der Informatik nicht verlässlich war.

V.II. KLINIKINFORMATIONSSYSTEM IM KANTONSSPITAL BASEL-LANDSCHAFT AM STANDORT LIESTAL

Klinikinformationssysteme bieten aufgrund der sensitiven Natur der bearbeiteten Personendaten sowie der zahlreichen Schnittstellen innerhalb und ausserhalb des Spitals besondere Herausforderungen für den Datenschutz. Aus diesem Grund hat die ASD im Rahmen ihrer risikobasierten Kontrollplanung im Jahr 2015 entschieden, eine Kontrolle von Teilbereichen des Klinikinformationssystems des Kantonsspitals am Standort Liestal durchzuführen. Diese datenschutzrechtliche Kontrolle wurde Ende 2015 im Detail geplant und begonnen. Die Kontrolle vor Ort und der Schlussbericht zur Kontrolle folgten anfangs 2016.

Die im Januar 2016 durchgeführte Kontrolle vor Ort ergab zwölf Feststellungen zu dringlich zu behebenden Mängeln und dreizehn Schwachstellen, welche ein mittleres Risiko bergen. Dabei ging es um Themen wie Risikomanagement, Lösch- und Archivierungskonzepte, Berechtigungs- und Zugriffskonzepte sowie Nachvollziehbarkeit der Datenzugriffe. Ausserdem wurden da und dort organisatorische Regelungen als im Sinne von § 8 IDG angemessene Schutzmassnahmen deklariert, was die ASD angesichts der heutigen Möglichkeiten von technischen Schutzmassnahmen (privacy by design/by default) bemängelte.

Im Rahmen ihrer Prüftätigkeit ist die ASD jedoch auf keine Sachverhalte gestossen, welche darauf hingedeutet hätten, dass die Rechtmässigkeit und die Zweckbindung der Datenbearbeitung im Klinikinformationssystem (KIS) nicht gegeben wären. Allerdings fiel auf, dass das Bewusstsein für die rechtzeitige Klärung von Datenschutzfragen in Projekten (Vorabkontrolle) grundsätzlich nur beim Datenschutzbeauftragten des Kantonsspitals vorhanden war.

VI. STELLUNGNAHMEN

Das Verfassen von Stellungnahmen stellt nach wie vor einen wichtigen Teil der Aufgaben der ASD dar. Im Berichtsjahr mussten wir erneut feststellen, dass wir Unterlagen zu Vernehmlassungen des Bundes mit einer Verspätung von bis zu einem Monat erhielten. Um sich mit der Materie auseinanderzusetzen blieb dann oft zu wenig Zeit. In solchen Situationen waren wir jeweils dankbar, wenn unser Verband «Privatim» schon etwas verfasst hatte, auf das wir uns beziehen konnten (vgl. Ziff. VII.IV.). Beim Verfassen von Stellungnahmen im Mitberichtsverfahren machten sich zudem unsere gekürzten Ressourcen bemerkbar, die eine sorgfältige Auseinandersetzung mit der Materie nur selten erlaubten. Dies vor allem dann, wenn mehrere Mitberichte auf einmal im Umlauf waren, zu denen wir etwas hätten sagen müssen. So wurden z.B. die Informatikverordnung, die Verordnung zum Projektmanagement und die Digitalisierungsstrategie im gleichen Zeitraum in das Mitberichtsverfahren gegeben, was sachlich durchaus sinnvoll sein kann. Im Interesse einer fundierten Stellungnahme wäre in solchen Fällen allerdings eine verlängerte Frist durchaus angebracht gewesen.

Inhaltlich äusserten wir uns u.a. zur Änderung der Kantonsverfassung und des Bildungsgesetzes, zur Hinterlegung von Vorsorgeaufträgen, zum Lohnsystem, zum Beschaffungswesen, zum Polizeigesetz, zur Schuladministration, zur Verordnung über Geoinformation, zum E-Government, zur SAP Zeitwirtschaft, zur Opferhilfe, zur Weiterentwicklung des Datenschutzrechts der Europäischen Union und des Europarates, zum E-Patientendossier, zu mobile computing, zur Verordnung betr. Kinder- und Jugendhilfe sowie zum Bedrohungsmanagement.

Und schliesslich äusserten wir uns auch zum Vorstoss Nr. 2015-418, der folgendes verlangt:

«Das Datenschutzgesetz verpflichtet die Fachstelle Datenschutz des Kantons auch zur Auskunft/Beratung von Stellen ausserhalb der kantonalen Verwaltung. Diese Tätigkeiten nehmen einen nicht unbedeutenden Teil der Arbeit der Fachstelle Datenschutz ein. Leider fehlt im Datenschutzgesetz die gesetzliche Grundlage, diese Beratungs-Dienstleistungen zu verrechnen, was negative Konsequenzen auf den Finanzsaldo der Fachstelle Datenschutz hat. Entsprechend wird beantragt: Die gesetzlichen Grundlagen für die Verrechnung der Dienstleistungen der Fachstelle Datenschutz an Externe sind zu schaffen.»

Da sich bereits abzeichnete, dass das übergeordnete Recht kaum eine Verrechnung von Leistungen der Datenschutzbehörden zulassen würde, beantragte die ASD die Überweisung der Motion als Postulat. Diesem Antrag wurde nicht stattgegeben. So wird die ASD im Rahmen der anstehenden Revision des IDG erklären müssen, weshalb das europäische Recht eine Gebührenerhebung bei Privaten nur äusserst eingeschränkt ermöglicht. Will der Kanton weiterhin Daten mit dem Ausland austauschen, ist er an diese Vorgaben direkt und indirekt gebunden. Zudem geht auch das revidierte Datenschutzgesetz des Bundes von einem kostenlosen Zugang aus.

VII. ÖFFENTLICHKEITSARBEIT UND SCHULUNGEN

VII.I. ÖFFENTLICHKEITSARBEIT

Die ASD beantwortete elf Anfragen von Medienvertretern. Es waren u.a. Fragen zum Sperrrecht, zur Anzahl der Anfragen, zur Herausgabe von Kontrollberichten, zur Videoüberwachung, zur Budgetkürzung, zur Vernichtung von Datenträgern und zum Internet-Amtsblatt. Für proaktive Öffentlichkeitsarbeit fehlte die Zeit.

VII.II. SCHULUNGEN

Auch im vergangenen Jahr hat die ASD wieder Schulungen allgemeiner und themenbezogener Art abgehalten. Traditionsgemäss wurden die KV-Lernenden des Kantons im Rahmen der überbetrieblichen Kurse in den Grundsätzen des kantonalen Datenschutzes, aber auch des Öffentlichkeitsprinzips unterrichtet. Dabei wurde je eine Veranstaltung für die duale Lehre und die Wirtschaftsmittelschule durchgeführt. Im Rahmen ihrer Ausbildung wurde zudem eine Veranstaltung für die Polizeiaspiranten und -aspirantinnen durchgeführt. Ebenfalls der Tradition folgend wurden die vom Personalamt angebotenen Weiterbildungskurse zu den Themen Datenschutz und Öffentlichkeitsprinzip von der ASD durchgeführt, wobei die beiden Kurse im Berichtsjahr zusammengelegt wurden. Themenspezifisch war die ASD bei der Regionalen Arbeitsvermittlung RAV zu Gast. Schulungen, welche auf einen spezifischen Bereich näher eingehen, können sehr effektiv sein, da viel präziser auf die in der Praxis relevanten Fälle eingegangen werden kann. Allerdings bedeuten sie auch einen bedeutend höheren Aufwand, den die ASD gegenwärtig kaum leisten kann.

VIII. KANTONALE, NATIONALE UND INTERNATIONALE ZUSAMMENARBEIT

VIII.I. ZENTRALE INFORMATIK (ZI) UND SICHERHEITSBEAUFTRAGTE

Die ASD traf sich wie bereits im letzten Berichtsjahr in regelmässigen Abständen mit dem Leiter ZI und dessen Stellvertreter. Diese äusserst wertvollen Treffen dienten dem Informationsaustausch zu Informatikprojekten, der Abstimmung der datenschutzrechtlichen Vorabkontrolle mit der Projektmanagementmethode HERMES und nicht zuletzt auch dem regelmässigen Austausch, um Handlungsbedarf auf beiden Seiten zu erkennen. Die Praxis hat sich bereits in den Vorjahren bewährt und trägt zur effizienten Bearbeitung der Datenschutz- und Informationssicherheitsthemen bei.

Die ASD nahm zudem auch 2016 in beratender Funktion an den Sitzungen der Sicherheitsbeauftragten teil. Sie nahm in ihrer Rolle u.a. Stellung zu Konzepten betreffend sichere Entsorgung von Datenträgern, zum sicheren Informationsaustausch, zu einer Studie Verschlüsselung und lieferte Beiträge zum revidierten Informationssicherheitskonzept und einem Fact-Sheet zur Informationssicherheit für Endanwender/innen.

Im Rahmen ihrer Beratungsdienstleistungen empfahl die ASD dem Kantonalen Sicherheitsbeauftragten, mit einem «Grundschutzkatalog» verbindliche Standard-Sicherheitsmassnahmen zu definieren, welche es beim Schutz von Informationen im Minimum zu beachten gilt. Die zentrale Umsetzung des daraufhin entstandenen «Grundschutzkatalogs» wurde im Berichtsjahr unter Federführung des Kantonalen Sicherheitsbeauftragten gestartet. An den Sitzungen der Sicherheitsbeauftragten wurde auch die dezentrale Umsetzung des verabschiedeten «Grundschutzkatalogs» regelmässig thematisiert. Die konkrete Umsetzung ist jedoch noch nicht in allen Direktionen eingeplant.

Zusammenfassend ist festzustellen, dass sich die Fachleute der IT-Risiken oft durchaus bewusst sind. Sie haben jedoch ungenügende Mittel, um diesen Risiken adäquat zu begegnen.

VIII.II. FINANZKONTROLLE

Die Revisionsleitung Informationssicherheit und Datenschutz hat auch im Jahr 2016 den Kontakt mit den Revisoren der Finanzkontrolle gesucht und sie zu den erfolgten und geplanten Kontrollen informiert. Die ASD versuchte so, Synergien zu nutzen und zu vermeiden, dass bei einer Behörde zwei Kontrollen im selben Jahr durchgeführt werden. Eine Kontrolle wurde auf Basis dieses Austauschs verschoben, wobei nicht übersehen werden darf, dass sich der Fokus der Kontrollen unterscheidet und dieselbe Feststellung aufgrund dessen zu anderen Empfehlungen führen kann.

VIII.III. ARBEITSGRUPPE DATENSCHUTZ DER KONFERENZ DER KANTONSREGIERUNGEN (KDK)

Die ASD war in einer Arbeitsgruppe der KdK vertreten, die sich mit der anstehenden Revision des Datenschutzrechts beschäftigte. Ergänzend arbeitete sie in einer interkantonalen Arbeitsgruppe mit (vgl. II.IV.). Die Zusammenarbeit mit anderen Behörden war einmal mehr sehr hilfreich.

VIII.IV. PRIVATIM

Im Berichtsjahr fanden zwei Plenumsveranstaltungen der Vereinigung der schweizerischen Datenschutzbeauftragten statt. Die Mitglieder befassten sich wie meist mit aktuellen Datenschutzthemen. Zudem unterstützte der Verband das Symposium on Privacy and Security, das sich mit der Frage des Datenschutzes in der digitalisierten Welt beschäftigte. Die Vereinsarbeit wird von ein paar wenigen Kantonen getragen, die viel für den Datenschutz leisten. Im Gegenzug haben sie oft einen gewissen Wissensvorsprung und können unter anderem so von der Vereinsarbeit profitieren. Als die Frage der Vergütung für Vorstandsarbeit diskutiert wurde, hat sich die ASD dagegen ausgesprochen, da die Vereinsbeiträge aus Steuergeldern der einzelnen Kantone

finanziert werden und diese – nach Auffassung der ASD – nicht für die Vergütung einzelner Vorstandsmitglieder resp. Datenschutzbehörden genutzt werden sollten. Es wäre vielmehr wünschenswert, dass alle Datenschutzbehörden über die für die Mitarbeit notwendigen Ressourcen verfügten.

Der interkantonale Austausch in der Arbeitsgruppe «Information and Communication Technology (AG ICT)» wurde auch im Berichtsjahr gepflegt, um Synergien zu nutzen. Die AG ICT verfasste ein Merkblatt zur Vernichtung elektronischer Daten. Zudem definierte sie ein Vorgehen zur Nutzung von interkantonalen Synergien bei der Auditierung und konnte dieses Vorgehen bereits einmal bei der Kontrolle einer Informatiklösung anwenden, welche mehrere Kantone einsetzen.

VIII.V. SIS-KOORDINATIONSGRUPPE

Die SIS-Koordinationsgruppe traf sich zwei Mal, um die Erfahrungen mit SIS-Kontrollen auszutauschen und sich über die Entwicklungen auf europäische Ebene zu informieren. Dabei waren die Gesetzgebungsarbeiten der EU und des Europarats regelmässig Gegenstand der Diskussion.

IX. ÖFFENTLICHKEITSPRINZIP

Ein häufig zu hörendes Argument gegen die Einführung des Öffentlichkeitsprinzips, also des Rechts auf Zugang zu bei Behörden vorhandenen Informationen, war die Befürchtung, dass die Verwaltung durch eine Flut von Gesuchen überschwemmt werden könnte. Diese Befürchtungen bewahrheiten sich in den wenigsten Fällen, und nach den der ASD vorliegenden Informationen stimmt diese Aussage auch für den Kanton Basel-Landschaft nicht. Die Zahl der Anfragen an die ASD im Zusammenhang mit dem Recht auf Zugang zu Informationen bewegte sich im Berichtsjahr nach wie vor auf überschaubarem Niveau. Allerdings führt die ASD anders als in anderen Kantonen keine Schlichtungen durch, sodass sie nicht über alle diesbezüglichen Verfahren informiert ist. Die Untersuchungen des Bundes im Rahmen der Evaluation anlässlich des 10. Jahrestages des Öffentlichkeitsgesetzes zeigen überdies auch, dass es eine gewisse Anlaufzeit brauchte, bis sich dieses Instrument voll entfaltete. So stiegen die Gesuchzahlen im Bund seit 2006 stetig an. Auch in unserem Kanton ist eine stetige Zunahme der Gesuche – auf tiefem Niveau – festzustellen. Zudem haben die Direktionen vereinzelt noch Mühe, zwischen einem Gesuch um Einsicht in die eigenen Daten nach Datenschutzrecht und einem Gesuch um Zugang zu Informationen nach dem Öffentlichkeitsprinzip zu unterscheiden. Im zweiten Fall dürfen unter gewissen Umständen Gebühren erhoben werden. Der Zugang zu den eigenen Daten muss jedoch grundsätzlich kostenlos möglich sein.

Die Themen, welche an die ASD herangetragen wurden, betrafen Dokumente und Informationen aus ganz verschiedenen Bereichen. So waren wieder einmal Schulrats- und Gemeinderatsprotokolle ein Thema, es wurde Einsicht in Baugesuchunterlagen ausserhalb der gesetzlichen Auflagefrist verlangt, oder es wurden Statistiken betreffend gewisser Asylsuchenden in den Gemeinden gefordert. In einem Fall wollte eine Gemeinde eine Information von einer kantonalen Behörde auf dem Weg des Öffentlichkeitsprinzips erlangen. Dazu ist zu sagen, dass dieser Weg einem öffentlichen Organ nicht offensteht, sondern Privaten vorbehalten ist.

Wenn aus den Anfragen, die an die Aufsichtsstelle gerichtet wurden, ein Trend ermittelt werden kann, dann ist es – wenig überraschend – jener, dass häufig dann Unklarheiten bestehen, wenn die verlangten Informationen Personendaten (mit-)betreffen. Denn grundsätzlich ist das Öffentlichkeitsprinzip nicht gedacht für die Bekanntgabe von Personendaten, dazu gibt es im datenschutzrechtlichen Teil des IDG die §§18 und 19. Und trotzdem gibt es Fälle, in welchen eine Information mit Personendaten von öffentlichem Interesse sein kann. Auf Bundesebene besteht dazu eine reichhaltige Rechtsprechung, welche regelmässig auf eine Interessenabwägung zwischen dem öffentlichen Interesse der All-

gemeinheit und den privaten Interessen der betroffenen Personen hinausläuft. Ein weiteres Thema war wiederholt die Frage der Anonymisierbarkeit von Informationen. Rechtsprechung zu diesem Punkt gibt es in unserem Kanton allerdings noch nicht. Allerdings hat das Appellationsgericht des Kantons Basel-Stadt in einem Entscheid vom 2. Dezember 2016 die (auch bei uns geltende) strikte Anonymisierungspflicht bejaht und den Zugang zu den Dokumenten unter anderem gestützt darauf verweigert, weil das Dokument nicht anonymisierbar war.[7] Dieses Urteil wurde inzwischen ans Bundesgericht weitergezogen. Aufgrund der Tatsache, dass die IDG der Beiden Basel fast identisch sind, wird der Entscheid des Bundesgerichts auch für den Kanton Basel-Landschaft von Bedeutung sein.

7] Urteil VD 2015.20, Erwägung 5.1

Angekommen ist das Öffentlichkeitsprinzip beim Kantonsgericht aber trotzdem. In einem Entscheid vom 10. August 2016[8] hatte das Gericht zu beurteilen, ob Zugang zu einem Altlastenbericht gegen den Willen der betroffenen Grundeigentümer gewährt werden müsse. Dieser Altlastenbericht hatte in einer Gemeinde eine Rolle bei der Entscheidungsfindung für den Standort eines Hochwasserrückhaltebeckens gespielt. Die angehörten Grundeigentümer machten geltend, einer Herausgabe stünden überwiegende private Interessen entgegen, insbesondere bestehe die Gefahr einer Wertminderung der belasteten Grundstücke. Die ASD war in dieser Sache zuvor im Verfahren vor dem Regierungsrat um eine Meinungsäusserung gebeten worden, und hatte unter anderem darauf hingewiesen, dass eine fehlende Einwilligung der betroffenen Dritten für sich allein genommen keinen Abweisungsgrund darstelle, sondern dass die auf dem Spiel stehenden Interessen gegeneinander abgewogen werden müssten. Anders als der Regierungsrat kam das Kantonsgericht in seiner Interessenabwägung zum Schluss, dass in diesem Fall die öffentlichen Interessen die privaten zu verdrängen vermochten und gewährte den Zugang. Beachtenswert in diesem Zusammenhang ist auch, dass die Angelegenheit den Anwendungsbereich der Aarhus-Konvention[9] betraf, welche für die Schweiz am 1. Juni 2014 in Kraft getreten ist. Diese Konvention sieht für den gesamten Umweltbereich das Öffentlichkeitsprinzip vor. Damit sind in diesem Bereich auch jene Kantone dem Öffentlichkeitsprinzip unterworfen, die es in der kantonalen Gesetzgebung (noch) nicht verankert haben. Den Kanton Basel-Landschaft betrifft dies nur insoweit, als im Zweifelsfall die Aarhus-Konvention zur Auslegung des IDG herangezogen werden kann, so wie dies auch das Kantonsgericht getan hat.

8] https://www.baselland.ch/politik-und-behorden/gerichte/rechtsprechung/kantonsgericht/rechtsgebiet/datenschutz

9] SR 0.814.07

Ähnlich wie der Datenschutz wird somit auch die Transparenz der Verwaltung zunehmend auch international standardisiert. Der EGMR hat dazu in einem Urteil entschieden, dass das Recht auf Zugang zu Informationen unter gewissen Bedingungen direkt auf Art. 10 Abs. 1 EMRK, das Recht auf freie Meinungsäusserung, gestützt werden kann und somit ein Menschenrecht darstellt.[10]

10] http://hudoc.echr.coe.int/eng#{«itemid»:[«001-167828»]}

X. AUSBLICK

Die Digitalisierung der Gesellschaft schreitet rasch voran. Mobile Computing, E-Health und personalisierte Medizin, elektronische Stellenbewerbungen, Big Data, Social Media, E-Tax, E-Government, Cloud-Computing, Deep-Learning, Internet der Dinge, Computer-Implantate, digitale Schulverwaltung, 3D-Druck etc. gehören zum Alltag. Langsam aber stetig entwickelt sich auch die Robotertechnik, welche die Gesellschaft noch stärker verändern wird. Kaum jemand kann mehr abschätzen, wohin die Reise geht und wie sich die Entwicklungen gesellschaftspolitisch und rechtlich begleiten lassen. Was wird mit den unzähligen persönlichen Daten in Zukunft geschehen? Wie weit geht künstliche Intelligenz? Was wird geschehen, wenn vernetzte Informations- und Kommunikationstechnologien inskünftig miteinander kommunizieren? Wo bleibt der Mensch und seine Fähigkeit, ethische Fragen zu stellen? All diese Aspekte haben auch mit Datenschutz zu tun. Es wird aber nicht genügen, Datenschutzbestimmungen zu erlassen und Datenschutzbehörden einzusetzen, die dafür Sorge tragen sollen, dass die Persönlichkeitsrechte der Bürgerinnen und Bürger auch in der modernen digitalen Gesellschaft gewahrt werden, dass Gesetze eingehalten werden. Selbst wenn die Datenschutzbehörden genügend Ressour-

cen hätten und als Experten wahrgenommen und gehört würden, wird deren Einsatz in Zukunft nicht mehr als ein Tropfen auf den heissen Stein sein können. Mit Datenschutz alleine werden sich die zentralen Fragen der digitalen Gesellschaft nicht lösen lassen. In Zukunft wird es deshalb multidisziplinäre Instanzen brauchen, die über Expertise in Recht, Ethik, Politik, Soziologie, Technik etc. verfügen.

Auf kantonaler Ebene wird im nächsten und übernächsten Jahr das IDG an das europäische Datenschutzrecht und an das Datenschutzrecht des Bundes angepasst werden müssen. Damit soll die Stärkung der Wirkung des Gesetzes und der Rechte der betroffenen Personen erreicht werden. Es werden begriffliche Änderungen vorgenommen werden müssen. Zudem muss das verantwortliche Organ nachweisen können, dass es die Datenschutzbestimmungen einhält. Weiter muss es bei jedem Vorhaben eine Datenschutz-Folgeabschätzung durchführen, die u.a eine Risikobewertung enthalten muss. Informationspflichten der Datenbearbeiter werden eingeführt, und sie werden verpflichtet, der ASD Datenschutzverletzungen anzuzeigen. Ferner soll eine Beschwerde an die Datenschutzbehörde möglich werden. Zudem wird im Gesetz festgeschrieben, dass die Datenschutzbehörde durch eine in Datenschutzfragen ausgewiesene Fachperson geleitet werden muss. Und last but not least werden die Leistungen der Datenschutzbehörde für die betroffenen Personen unentgeltlich sein.

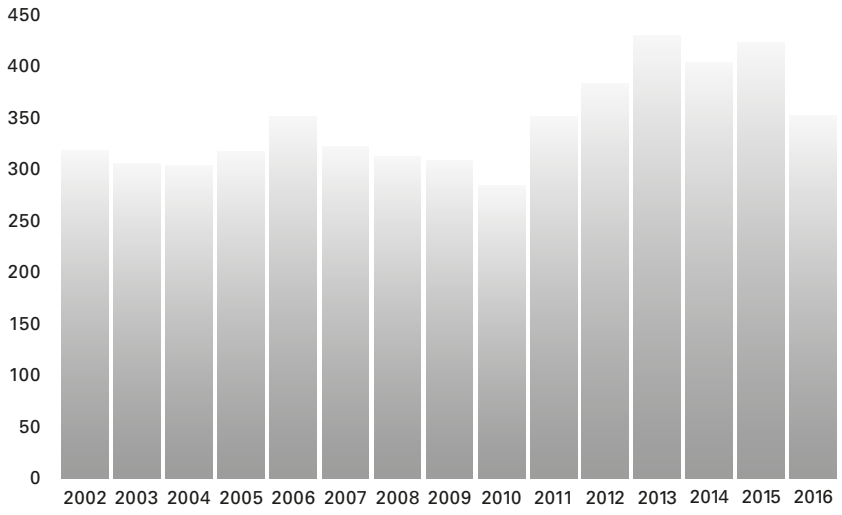
Ob diese Massnahmen zur geforderten Stärkung der Betroffenenrechte beitragen können, wird die Zukunft zeigen. Ohne zusätzliche Ressourcen bei allen Datenschutzbehörden wird das Gesetz weiterhin in weiten Teilen nicht umgesetzt werden. Nichts zu tun, ist aber keine Option, denn der Wandel hat schon längst begonnen. Ob es gelingt, die digitale Zukunft so zu gestalten, dass die Gesellschaft als Ganzes davon profitiert und die Menschenwürde erhalten bleibt, ist letztlich eine politische Frage.

XI. PERSÖNLICHER SCHLUSSPUNKT

«Wer nichts zu verbergen hat, hat nichts zu befürchten.» Diese Aussage kennen Sie sicher. Stimmt sie für Sie, oder haben am Ende auch Sie ein Geheimnis? Haben Sie vielleicht auch Jugendsünden begangen, an die Sie heute lieber nicht mehr denken? Oder haben Sie auch schon gedacht «zum Glück hat mich niemand gesehen»? Wir alle haben wohl unsere Geheimnisse. Wollen wir nicht auch selbst darüber entscheiden, wer diese Geheimnisse erfahren darf? Die Aufsichtsstelle Datenschutz setzt sich seit Jahren dafür ein, dass Sie grundsätzlich selbst bestimmen können, wer was über Sie wissen darf. Selbstverständlich findet die «Geheimniskrämerei» dort ihre Grenzen, wo der Staat Angaben zu Ihrer Person benötigt, damit er seine gesetzliche Aufgabe überhaupt erfüllen kann. Stellen Sie sich eine Welt ohne Privatsphäre vor. Würden Sie Ihre Meinung noch frei äussern, wenn Sie befürchten müssten, Sie würden abgehört? Oder wie würden Sie stimmen und wählen, wenn dies immer öffentlich und unter Namensnennung geschehen müsste? Sind Sie nicht auch der Meinung, dass es intime Dinge gibt, die niemanden ausserhalb ihres Kreises etwas angehen, oder würden Sie gerne in einem Glashaus wohnen? Wenn wir eines Tages nichts mehr verbergen dürfen, haben wir am Ende vielleicht doch etwas zu befürchten. Und wenn dereinst Roboter über uns entscheiden oder uns am Lebensende pflegen sollen, möchten wir vielleicht doch noch eine Wahl haben. Mit diesen Gedanken verabschiede ich mich per Ende 2017 vom Kanton Basel-Landschaft und danke meinem hervorragenden und stets loyalen Team, meinen Kolleginnen und Kollegen im In- und Ausland sowie all jenen Menschen, die mich in den letzten 16 Jahren wertschätzend, motivierend und offen für die Anliegen des Datenschutzes und der digitalen Gesellschaft begleitet haben.

ANHANG

GESCHÄFTE



ART DER GESCHÄFTE