BASEL LANDSCHAFT

Vorlage an den Landrat

Titel:	**Tätigkeitsbericht 2015 der Aufsichtsstelle Datenschutz**
Datum:	23. Juni 2016
Nummer:	2016-040_09
Bemerkungen:	**Verlauf dieses Geschäfts**

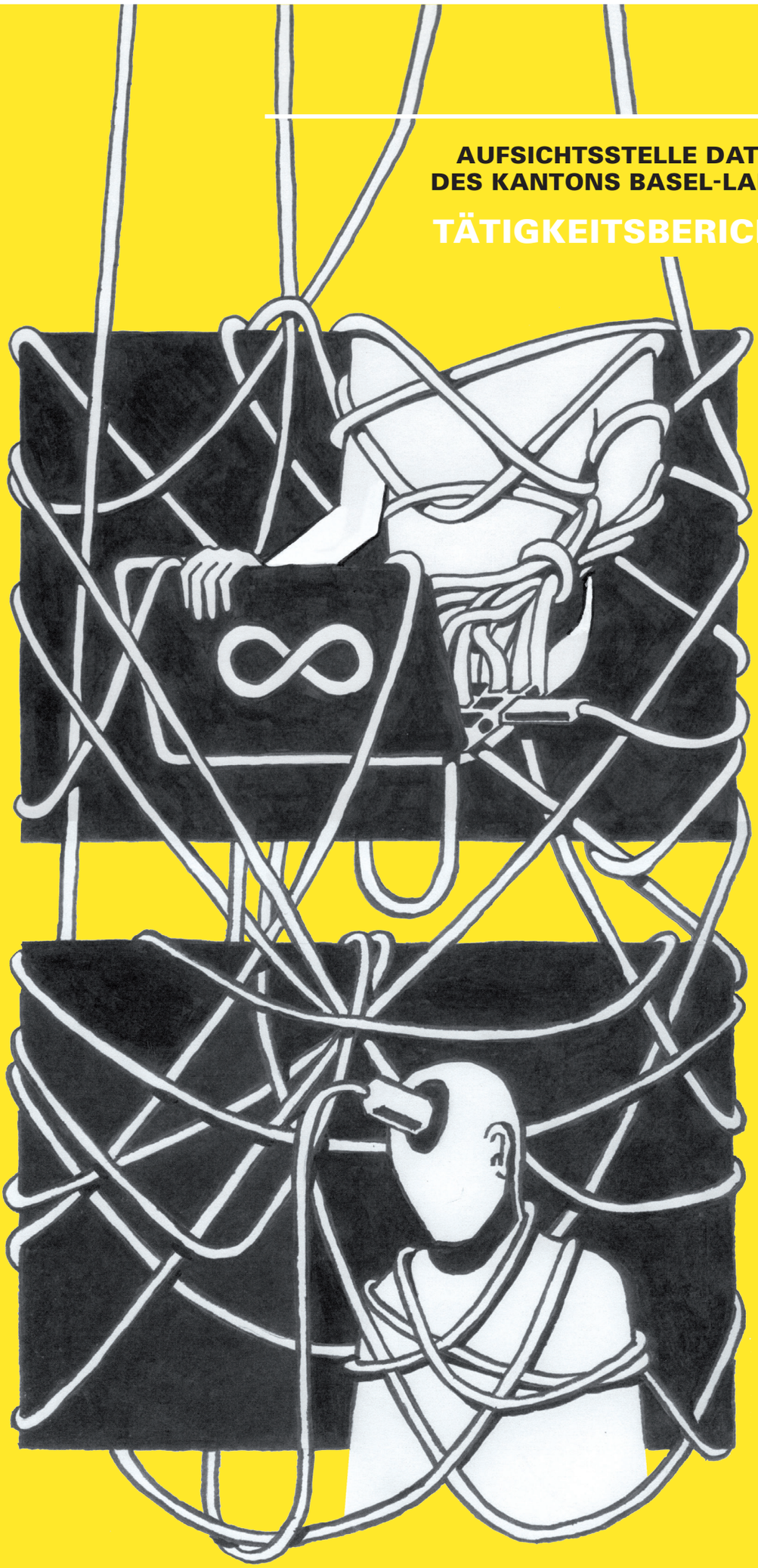
Links:

- Übersicht Geschäfte des Landrats
- Hinweise und Erklärungen zu den Geschäften des Landrats
- Landrat / Parlament des Kantons Basel-Landschaft
- Homepage des Kantons Basel-Landschaft

AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

TÄTIGKEITSBERICHT 2015

2016/040-09



AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragte:	Ursula Stucki
Stv. Datenschutzbeauftragter:	Tobias Schnelli
Akademische Mitarbeitende:	Priscilla Dipner-Gerber
	Thomas Held
	Michael Schnyder
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 2015

I.I. DER AUFTRAG DER DATENSCHUTZ-BEHÖRDE

Jede Person hat das Recht auf Schutz vor unrechtmässiger staatlicher Datenbearbeitung. Kaum jemand wird jedoch in der Lage sein, selbst zu prüfen, ob der Staat die bei ihm vorhandenen Daten rechtmässig nutzt und die Bevölkerung vor Missbrauch schützt. Aus diesem Grund gibt es die Aufsichtsstelle Datenschutz (ASD). Sie soll die Bevölkerung in der Wahrnehmung ihrer Rechte unterstützen, die Rechtmässigkeit der staatlichen Datenbearbeitung kontrollieren und vorbeugend einem Datenmissbrauch entgegenwirken.

Die Aufsichtsstelle hat gemäss § 40 IDG folgenden Auftrag. Sie

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

I.II. DAS WESENTLICHE IN KÜRZE

2015 eröffnete die ASD 424 neue Dossiers. In Erfüllung ihres gesetzlichen Auftrags startete sie – im Rahmen ihrer risikobasierten rollenden Planung – zwei Kontrollen und beendete deren zwei. Zusätzlich fand im Berichtsjahr eine anlassbedingte Kontrolle statt. Sie prüfte, zum Teil mehrfach, 15 Projekte, die ihr im Rahmen der Vorabkontrolle in verschiedenen Phasen vorgelegt wurden, nahm 206 Fragen von Behörden entgegen (198 zum Datenschutz, 8 zum Öffentlichkeitsprinzip), befasste sich mit 70 Anfragen von Privaten (68 zum Datenschutz, 2 zum Öffentlichkeitsprinzip), prüfte 53 Einladungen zur Stellungnahme, führte 7 Schulungen durch und erledigte diverse administrative Arbeiten, die von Jahr zu Jahr aufwendiger werden.

Im Berichtsjahr entwickelte die ASD den Bereich der Vorabkontrolle weiter und verlieh dem präventiven Handeln der Datenschutzbehörde dadurch mehr Gewicht. Ziel dieser zentralen Aufgabe ist es, allfällige Fehlentwicklungen in Projekten rechtzeitig zu erkennen und die Verantwortlichen darauf aufmerksam zu machen, damit nachträgliche kostenintensive Nachbesserungen vermieden werden können.

Die Zusammenarbeit mit unterschiedlichen Organen, die sich mit den ähnlichen Themen beschäftigen, war auch im Berichtsjahr wieder wichtig und hilfreich. Die ASD nahm unter anderem an zwei Plenarversammlungen der schweizerischen Datenschutzbeauftragten teil und war in der schweizerischen Schengen-Koordinationsgruppe sowie der Arbeitsgruppe Datenschutz der Konferenz der Kantonsregierungen (KdK) vertreten. Zudem arbeitete sie in der schweizerischen Arbeitsgruppe ICT mit und tauschte sich regelmässig mit Datenschutzbeauftragten anderer Kantone und den kantonalen Sicherheitsbeauftragten aus.

Nachdem die Datenschutzbehörde 2013 zusätzliche finanzielle Mittel (Fr. 150 000.–) erhalten hatte und damit erstmals in ihrer Geschichte alle gesetzlichen Aufträge im Ansatz erfüllen konnte, beschloss die Mehrheit des Landrats am 16. Dezember 2015, die Mittel der Datenschutzbehörde um rund 22 % zu kürzen (Fr. 197 000.–). Damit wurde die in den vergangenen Jahren geleistete Aufbauarbeit in Richtung einer professionellen und effizienten Kontrollbehörde ohne sachliche Auseinandersetzung oder Begründung infrage gestellt. Die Mittelkürzung , die sich marginal auf die Finanzlage des Kantons auswirken wird (rund 0.008 % des Gesamtbudgets), stellt die Datenschutzbehörde vor grosse Probleme. Sie wird unter anderem einen Abbau von personellen Ressourcen und damit einen Leistungsabbau zur Folge haben. Die ASD ist damit erneut in der schwierigen Lage, dass sie ihren umfassenden gesetzlichen Auftrag kaum

mehr erfüllen kann. Die Datenschutzbeauftragte wird bei der Umsetzung der landrätlichen Vorgaben alle ihre Aufgaben prüfen und den Sparstift dort ansetzen, wo analoges Fachwissen bei den öffentlichen Organen vorhanden ist oder sein müsste. Dies wird voraussichtlich für die Verwaltung einen spürbaren Leistungsabbau zur Folge haben.

II. AUSGEWÄHLTE THEMEN 2015

II.I. IMPLEMENTIERUNG DER VORABKONTROLLE

Mit der 2008 gesetzlich eingeführten Vorabkontrolle sollen die Anforderungen des Datenschutzes rechtzeitig, noch in der Konzeptphase, qualitätssichernd in das Projekt einfliessen. Die Vorabkontrolle bringt eine Win-win-Situation für Projektauftraggeber und Datenschutz, indem mit dem Aufzeigen konkreter Datenschutzanforderungen in der Konzeptphase aufwendigere Nachbesserungen bei der Umsetzung vermieden werden können. Und dies, bevor bereits grosse Investitionen getätigt wurden. Ist ein Projekt erst einmal in der Realisierungsphase, sind Unterlassungsfehler – wenn überhaupt – nur mit grossem (finanziellen) Aufwand zu korrigieren.

Trotz des offensichtlichen Nutzens wurden der ASD in der Vergangenheit lediglich vereinzelt Projekte zur Vorabkontrolle vorgelegt. Das lag sicher auch daran, dass die ASD bis Mitte 2014 nicht über die erforderlichen Fachleute verfügte, um die öffentlichen Organe ausreichend für die Vorabkontrolle zu sensibilisieren und mit methodischen Grundlagen zu unterstützen.

Im April 2015 publizierte die ASD einen Leitfaden, welcher sowohl den Projektverantwortlichen als auch den verantwortlichen Organen als Unterstützung bei der Triage und der Einbettung der Vorabkontrolle in den Projektablauf dient. Dabei wurde grosser Wert darauf gelegt, auf die im Kanton bereits standardisierte Projektmethode HERMES aufzubauen. Keine der datenschutzrechtlich zu prüfenden Angaben und Dokumente müssen «nur» für diese Vorabkontrolle erarbeitet werden, vielmehr sind sie wesentliche Bestandteile eines geordneten Projektmanagements und sollten im Laufe eines Informatikprojektes sowieso erstellt werden. Beispiele für solche Dokumente sind die Rechtsgrundlagenanalyse, die Schutzbedarfsanalyse und das sogenannte ISDS[1]-Konzept.

Unsere Erfahrungen zeigen allerdings, dass beim Projektmanagement trotz einer geltenden Verordnung[2] noch ein Vollzugsdefizit besteht. Im Rahmen der datenschutzrechtlichen Vorabkontrolle der Angemessenheit von Massnahmen zum Schutz der Informationen (gemäss § 8 IDG) stellte die ASD im Berichtsjahr verschiedentlich fest, dass kurz vor der Inbetriebnahme einer Anwendung weder der Schutzbedarf der Informationen erhoben noch eine entsprechende Konzeption zu deren Schutz erstellt wurde. In mehreren Projekten waren auch die Verantwortlichkeiten bis kurz vor der Realisierung ungeklärt. Dies betraf sowohl die Verantwortlichkeit für die Datenbearbeitung gemäss § 6 IDG als auch die Zuständigkeit für die Analyse der bestehenden oder zu schaffenden Rechtsgrundlagen. In einem Fall (in welchem auch besondere Personendaten bearbeitet werden) wurde die «Konzeption» gar erst nach Inbetriebnahme einer Cloudlösung nachdokumentiert. Dieses Vorgehen ist nicht nur aus Datenschutzoptik kritisch zu beurteilen. Es besteht das Risiko, dass ein Produkt oder ein Provider ausgewählt wird, bevor die Anforderungen klar sind, und letztlich die Anbieter die Geschäftsprozesse und das Schutzniveau bestimmen. Damit sind auch finanzielle und submissionsrechtliche Aspekte berührt.

Eine weitere Schwierigkeit in der Vorabkontrolle zeigte sich im Zusammenhang mit der notwendigen Analyse der Rechtsgrundlagen (HERMES Standard und § 9 IDG). Die ASD wies mehrfach darauf hin, dass die Beseitigung allfälliger Gesetzeslücken in Projekten essenziell ist. Den Projektorganisationen steht jedoch vielfach kein juristisches Know-how zur Verfügung. Dies führte vielfach dazu, dass Projekte inhaltlich ungenügend auf ihre Rechtmässigkeit überprüft wurden. Oftmals bestand eine Erwartungshaltung, dass die ASD diese Lücke schliesse. Doch die Fachkenntnisse betreffend Aufgaben, Tätigkeiten und Arbeitsprozesse der öffentlichen Organe, zu welchen die Rechtsgrundlagen

1] ISDS = Informationssicherheit und Datenschutz

2] Verordnung vom 30. Oktober 2012 zum Projektmanagement (SGS 140.15)

analysiert werden müssen, haben nur die öffentlichen Organe selbst. Die ASD kann diese Kenntnisse weder inhaltlich noch ressourcenmässig ersetzen. Die ASD versuchte diesem Zustand entgegenzuwirken, indem sie wiederholt über diese Schwierigkeiten informierte (Fachgruppe Informatik, ITO-Rat, Sicherheitsbeauftragte). Die Sicherheitsbeauftragten der Direktionen bilden eine wichtige Schnittstelle in der Vorabkontrolle und wurden auch im Berichtsjahr über die ihre Projekte betreffenden Vorabkontrollen laufend informiert.

Im Berichtsjahr sind bei der ASD fünfzehn Projekte zur Prüfung einer Vorabkontrolle eingegangen. Bei sechs davon wurde keine Vorabkontrolle durchgeführt, da entweder das Risiko als klein eingestuft wurde (zwei) oder sie zu spät im Projektablauf eingegangen waren (vier). Gegen Ende des Berichtsjahres zeigte sich ein stärkeres Bewusstsein für die rechtzeitige Kontaktaufnahme betreffend Vorabkontrolle. Dies ist sicher auch auf die verschiedenen Awareness-Kampagnen der ASD sowohl in Entscheidungsgremien als auch auf Stufe der Projektleitenden zurückzuführen.

Schwerpunktmässig zeigte sich in den Vorabkontrollen Handlungsbedarf betreffend strukturiertes Vorgehen, Umsetzung der kantonalen Vorgaben im Bereich ISDS, Berechtigungskonzepte und Outsourcingverträge.

II.II. FEHLENDER EINBEZUG DER VERANTWORTLICHEN (INFORMATIONSEIGNER)

Die ASD hat bei verschiedenen Informatikprojekten festgestellt, dass diese ohne Einbezug der Informationseigner durchgeführt wurden. Das ist problematisch, weil die Informationseigner das gemäss § 6 IDG verantwortliche öffentliche Organ sind und nur sie in dieser Rolle den Schutzbedarf der bei ihnen vorhandenen Daten kennen. Wenn sie bei einem Projekt nicht einbezogen werden, können keine dem Schutzbedarf angemessenen Massnahmen für die Informationssicherheit geplant und umgesetzt werden. Gerne wird die Verantwortung der Definition des Schutzbedarfs an die Informatik delegiert, indem nicht nur in Infrastrukturprojekten, sondern auch in Fachprojekten der Top-down-Ansatz verfolgt wird. Dies führt dazu, dass nicht der Schutzbedarf die technischen Massnahmen steuert, sondern die technischen Massnahmen den Umfang des tatsächlich gewährten Schutzes vorgeben.

Schwierig ist der Einbezug der Informationseigner bei Infrastrukturprojekten wie z.B. Multifunktionsprinting oder Mobile Device Management (MDM), weil diese Projekte nicht nur einzelne, sondern viele oder sogar alle Verwaltungseinheiten betreffen und deshalb potenziell die ganze Breite der Vertraulichkeitsklassen möglich ist (siehe Kapitel IV.). Trotzdem sollte es nicht versäumt werden, die Informationseigner in die Projekte einzubinden.

Auch bei der Festlegung der Berechtigungen wird der Einbezug der Informationseigner oft vergessen. Die Datenschutzbeauftragte begrüsst, dass die Informationssicherheitsbeauftragten die Hinweise der ASD aufgenommen und für 2016 eine Awarenesskampagne zum Thema «Rolle und Aufgabe der Informationseigner» geplant haben.

II.III. EINFLUSS DES EUROPÄISCHEN DATENSCHUTZES AUF DIE SCHWEIZ

Wenn die Aufsichtsstelle Datenschutz in regelmässigen Abständen einen Blick über die Grenze ins europäische Umland riskiert, um die dortigen Entwicklungen im Datenschutzrecht zu verfolgen, tut sie dies nicht aus rein akademischem Interesse oder gar, weil sie auf der Suche nach Arbeit ist. Vielmehr ist das Interesse dem Umstand geschuldet, dass die Rechtsprechung und -setzung auf europäischer Ebene stets einen Einfluss auf das hiesige Datenschutzrecht hatte und hat. Betrifft ein neuer Rechtsakt einen Bereich, der zwischen der Schweiz und den europäischen Partnern in bilateralen Verträgen geregelt ist, hat dieser sogar direkte Wirkung für Bund und Kantone, da in einem solchen Fall unsere Datenschutzgesetze dem neuen Regelungsinhalt angepasst werden müssen.

Grund genug, um an dieser Stelle die Entwicklungen auf europäischer Stufe, die zur Verabschiedung des sogenannten Datenschutzpaketes Ende 2015 führten, und deren mögliche Auswirkungen auf die Schweiz in aller Kürze darzulegen.

Im vergangenen Jahrzehnt ist die Menge der erhobenen (Personen-) Daten geradezu explodiert. Getrieben wurde dieser Sammeleifer von der technologischen Entwicklung. Im digitalen Zeitalter ist die Erhebung von Personendaten im grossen Stile ausserordentlich einfach geworden. Aber nicht nur Smartphone und Internet, Roboter und Sensoren erleichtern die Datensammlung, auch der Mensch selber trägt eifrig dazu bei. Facebook und Co. haben gezeigt, dass das Teilen von Informationen über das eigene Leben vielen Menschen ein grosses Bedürfnis ist. Doch mit der Zeit wurde auch klar, dass die Datenflut gewisse Probleme mit sich bringen kann. Wer weiss heutzutage schon, wo welche Daten über seine Person gespeichert sind? Wer kann auf diese Daten zugreifen? Zu welchen Zwecken werden sie verwendet? Wie sieht es mit dem Recht aus, diese Daten wieder zu löschen? Welche Regeln gelten überhaupt in welchem Land? Das sogenannte Recht auf «Informationelle Selbstbestimmung», der eigentliche Kern des Datenschutzes, wurde immer mehr infrage gestellt.

Bisher war für die Staaten der EU eine Datenschutzrichtlinie aus dem Jahr 1995 massgebend. Diese verpflichtete die einzelnen Staaten, die darin enthaltenen Bestimmungen in ihre nationalen Gesetze zu überführen. Dies führte zu einer uneinheitlichen Gesetzgebung im europäischen Datenschutz, ein Umstand, den sich einige der grossen Datenverarbeiter zunutze machten, indem sie ihre europäische Niederlassung in einem Staat gründeten, in welchem sie die «weichste» Gesetzgebung sahen.

All diese Entwicklungen führten Anfang dieses Jahrzehnts zur Einsicht, dass das europäische Datenschutzrecht modernisiert und vereinheitlicht werden müsse. Die Arbeiten wurden 2012 aufgenommen und waren von Anfang an von einem äusserst intensiven Lobbying begleitet. Viele Unternehmen sahen den freien Datentransfer über die Grenzen gefährdet und fürchteten strenge Verbraucherschutzregeln. Einen Kontrapunkt setzte dabei der europäische Gerichtshof, der bei einigen aufsehenerregenden Fällen (Google, Vorratsdatenspeicherung, Safe Harbor) stets zu Gunsten der Privatsphäre entschied.

Nach langen und zähen Verhandlungen einigten sich Ende 2015 die Europäische Kommission, der Europäische Rat sowie das Europäische Parlament auf eine Version der sogenannten «EU-Datenschutz-Grundverordnung». Sie wurde am 14. April 2016 vom europäischen Parlament formell verabschiedet. Die Grundverordnung wird für die EU-Mitgliedsstaaten direkt anwendbar sein.

Als zweiter Teil des europäischen Datenschutzpakets wurde ebenfalls Ende 2015 eine Richtlinie zum Datenschutz bei der Zusammenarbeit der Polizei und der Gerichte in Strafsachen verabschiedet. Diese Richtlinie regelt die Datenbearbeitung in jenem Bereich, der in der Datenschutz-Grundverordnung offengelassen wurde. Bezüglich der Definitionen und der Grundsätze wurden die beiden Rechtsakte aufeinander abgestimmt. Die Richtlinie ist nicht direkt anwendbar, sondern muss in die nationale Rechtsordnung überführt werden.

Die Grundverordnung regelt die Datenverarbeitung von Privaten und öffentlichen Organen. Ein Ziel dabei war die Stärkung der Rechte der betroffenen Personen. Vor allem durch verstärkte Informationspflichten sowie präzisere Regelungen zur Einwilligung in die Datenverarbeitung oder zur Löschung von Daten sollen die Personen in die Lage versetzt werden, die Hoheit über ihre persönlichen Informationen zurückzugewinnen und zu behalten. Zusätzlich wurden Regelungen geschaffen, welche die Verwendung von datenschutzfreundlicher Informationstechnologie vorschreiben («privacy by design», «privacy by default»). Für die Bearbeitung von Daten durch den Staat enthält die Grundverordnung unter anderem weitergehende Informationspflichten und die Pflicht zur Dokumentation von Datenbearbeitungen (Logging). Die Aufgaben der Aufsichtsbehörden werden erweitert, und es wird vorgeschrieben, dass der Zugang zu den Aufsichtsbehörden für die betroffenen Personen sowie die zuständigen Datenschutzverantwortlichen der öffentlichen Organe unentgeltlich gewährt werden muss.

Die Stossrichtung der Richtlinie zur Zusammenarbeit in Strafsachen ist grundsätzlich die gleiche, eben beschränkt durch den Anwendungsbereich. So sind ebenfalls umfassende Informationspflichten vorgesehen, die jedoch leichter eingeschränkt werden können, wenn es der Strafverfolgung dient. Die umfassende Pflicht der Strafverfolgungsbehörden zur Kooperation mit den Aufsichtsbehörden

wird ebenfalls festgeschrieben. Die betroffenen Personen erhalten klare Möglichkeiten, sich gegen eine vermutete unrechtmässige Datenbearbeitung zu wehren, sei es bei der Aufsichtsbehörde oder durch ein Gericht. Auch in der Richtlinie wird der Datensicherheit mehr Gewicht eingeräumt als bisher, so wurde zum Beispiel die Pflicht eingeführt, die Aufsichtsbehörde und die betroffenen Personen über Datenpannen und -verluste zu informieren.

Die Schweiz hat sich mit dem Beitritt zu Schengen/Dublin verpflichtet, neue oder veränderte Rechtsakte, welche die europäische Kommission als Teil des sogenannten Schengen-Besitzstandes erklären, zu übernehmen und in das nationale Recht zu überführen. Tut sie dies nicht, riskiert sie die Kündigung der Verträge. Für die Richtlinie hat die Kommission die Schengen-Relevanz erklärt. Bund und Kantone sind gegenwärtig am Prüfen, ob und in welcher Art sie der Erklärung Folge leisten wird. Es ist abzusehen, dass eine Überführung der Richtlinie für Bund und Kantone Änderungen auch auf Gesetzesstufe zur Folge haben wird. Erklärt sich die Schweiz dazu bereit, hat sie eine zweijährige Frist zur Anpassung des nationalen Rechts.

Für die Grundverordnung hat die Kommission die Schengen-Relevanz verneint. Die Schweiz ist demnach nicht unmittelbar gehalten, Anpassungen vorzunehmen. Allerdings erfolgt der Austausch von Daten in Staaten, denen von der EU ein adäquates Datenschutzniveau attestiert wurde, einfacher. Die EU wird also nach einer angemessenen Frist überprüfen, ob das datenschutzrechtliche Niveau in der Schweiz jenem der Grundverordnung vergleichbar ist. Bund und Kantone haben somit einen grossen Anreiz, sich auch für die Grundverordnung datenschutzrechtlich «fit» zu machen. Es ist deshalb auch kein Zufall, dass die Arbeiten zur Revision des Bundesdatenschutzgesetzes auf Bundesebene erst dann richtig in Angriff genommen wurden, als sich die Einigung auf europäischer Ebene abzuzeichnen begann.

Während insbesondere die Datenschutz-Grundverordnung in letzter Zeit in der Presse rege diskutiert wurde, hat man die ebenfalls anstehende Revision eines der ältesten Abkommen zu diesem Thema eher stiefmütterlich behandelt. Die Europarats-Konvention 108 von 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten wurde von der Schweiz 1998 ratifiziert. 2012 wurde eine Revisionsvorlage verabschiedet, danach wurde der Prozess allerdings auf Eis gelegt, um die oben erwähnten Gesetzgebungsprozesse abzuwarten. Nach der Verabschiedung der Grundverordnung wird nun erwartet, dass auch die Konvention in diesem Jahr noch in Kraft treten wird. Die Schweiz dürfte aller Voraussicht nach die Konvention ebenfalls ratifizieren. Auch die Änderungen der Konvention gehen – nicht überraschend – in die gleiche Richtung wie die beiden anderen Erlasse. So wird allgemein eine Erhöhung der Transparenz von Datenbearbeitung angestrebt, zum Beispiel durch bessere Auskunftsrechte und Meldungen bei Verstössen und Pannen.

Gesamthaft betrachtet liegt nun also auf europäischer Ebene ein mehr oder weniger harmonisch abgestimmtes Erneuerungspaket für den Datenschutz vor. Für den Kanton Basel-Landschaft bedeutet dies, dass in der nächsten Zeit die Bedeutung dieser neuen europäischen Rahmenbedingungen vertieft geprüft werden muss, um daraus die Erkenntnis zu ziehen, ob und wie das Informations- und Datenschutzgesetz sowie die relevanten Verordnungen allenfalls angepasst werden müssen.

II.IV. VERTRAULICHKEITSKLAUSELN UND ÖFFENTLICHKEITSPRINZIP

Verträge zwischen öffentlichen Organen und privaten Unternehmen gibt es zahlreiche. Vertragsklauseln, in denen die Vertragsparteien vereinbaren, über den Inhalt des Vertrages Stillschweigen zu bewahren, sind im Geschäftsverkehr ebenfalls gang und gäbe. Was passiert aber, wenn nun eine Person gestützt auf das Öffentlichkeitsprinzip Zugang zu einem Vertrag zwischen einem öffentlichen Organ und einem/einer Privaten fordert und in diesem Vertrag eine Geheimhaltungsklausel eingefügt wurde? Kann das öffentliche Organ gestützt auf diese Klausel den Zugang verwehren?

Seit dem 1. Januar 2013 gilt im Kanton Basel-Landschaft das Öffentlichkeitsprinzip. Es besagt, dass grundsätzlich jede Person ohne Nachweis eines beson-

deren Interesses einen Anspruch auf Zugang zu den Informationen hat, die bei einem öffentlichen Organ vorhanden sind (§ 23 Abs. 1 IDG). Dieser Anspruch gilt indessen nicht uneingeschränkt. Der Zugang zu den Informationen kann verweigert, eingeschränkt oder aufgeschoben werden in den in § 27 IDG aufgeführten Fällen. Dies können neben gesetzlichen Geheimhaltungspflichten überwiegende öffentliche oder private Interessen sein. Beispiele für überwiegende private Interessen sind Berufs-, Fabrikations- und Geschäftsgeheimnisse (§ 27 Abs. 3 Bst. b IDG). Ebenso soll geschützt werden, wer einer Behörde eine Information unter ausdrücklicher Zusicherung der Vertraulichkeit mitteilt (§ 27 Abs. 3 Bst. c IDG). Ob ein Grund für eine Verweigerung des Zugangs vorliegt, kann immer nur anhand des konkret infrage stehenden Dokumentes ermittelt werden.

Die Landratsvorlage zum IDG führt zu § 27 Abs. 3 Bst. c IDG Folgendes aus: «Der Anspruch auf Vertrauensschutz gebietet es, Informationen, die einem öffentlichen Organ freiwillig und nur unter der Voraussetzung der Geheimhaltung mitgeteilt wurden, grundsätzlich geheim zu halten. Könnten solche Informationen trotz Vertraulichkeits-Zusicherung jedermann bekannt gegeben werden, wären Private kaum mehr bereit, den Behörden freiwillig Informationen zu liefern.»[3]

Informations- und Datenschutzgesetze anderer Kantone sowie das Bundesgesetz über die Öffentlichkeit in Art. 7 Abs. 1 Bst. h[4] kennen ähnlich lautende Bestimmungen. Die Lehre und Rechtsprechung hat diese Bestimmung so ausgelegt, dass drei Voraussetzungen erfüllt sein müssen, damit dieser Einschränkungsgrund greifen kann. Erstens muss die Information dem öffentlichen Organ von einer Privatperson mitgeteilt worden sein, wobei hier durchaus auch eine juristische Person infrage kommt. Zweitens muss das öffentliche Organ die Vertraulichkeit ausdrücklich zugesagt haben, und drittens darf die Information nicht aufgrund einer vertraglichen oder gesetzlichen Verpflichtung abgegeben worden sein.[5] In den hier interessierenden Fällen sind die ersten zwei Voraussetzungen erfüllt, da es sich beim Vertragspartner um einen Privaten handelt und eine Geheimhaltungsklausel vereinbart wurde. Da jedoch eine vertragliche Beziehung vorliegt, ist die dritte Voraussetzung nicht erfüllt, womit eine Berufung auf § 27 Abs. 3 Bst. c IDG für eine Verweigerung nicht infrage kommt. Die Bestimmung ist somit gemäss Lehre und Rechtsprechung für Situationen gedacht, in denen eine Privatperson sozusagen aus «heiterem Himmel» von sich aus auf eine Behörde zukommt und ihr Informationen unter der Bedingung der Vertraulichkeit preisgibt. Die Behörde kommt demnach nur an die Information, wenn sie die Vertraulichkeit zusichert. Bei einer vertraglichen Situation ist dies anders, da sich hier zwei Parteien auf Augenhöhe begegnen. Liesse man die Berufung auf diesen Einschränkungsgrund zu, könnten die beiden Vertragsparteien an der Schnittstelle Privatwirtschaft/öffentliches Organ weite Teile des Öffentlichkeitsprinzips aushebeln, was nicht im Sinne des Gesetzgebers sein dürfte.[6] Denn es liegt auf der Hand, dass an der Kenntnis von Verträgen zwischen der Verwaltung und Privaten grundsätzlich ein gewisses öffentliches Interesse besteht, da damit regelmässig auch die Verwendung von Steuergeldern verknüpft ist.

Eine Geheimhaltungsklausel in den Vertrag aufzunehmen, bietet für das öffentliche Organ demnach die Gefahr eines Dilemmas. Unter Umständen verpflichtet es sich zu etwas, was zu halten es nicht imstande ist. Wird der Vertrag durch die Rechtsprechung öffentlich gemacht, wird das öffentliche Organ gleichzeitig vertragsbrüchig. Diese Situation ist unter dem Begriff der «Zusicherungsfalle» bekannt.[7]

Wir empfehlen demnach, auf die Aufnahme einer Geheimhaltungsklausel in Verträgen mit Privaten zu verzichten. Aus Fairnessgründen würde es sogar naheliegen, die Vertragspartnerin ausdrücklich auf den Umstand aufmerksam zu machen, dass der Vertrag Gegenstand eines Zugangsgesuches nach dem Öffentlichkeitsprinzip werden könnte.

Im Übrigen bedeutet die Tatsache, dass eine Verweigerung oder Einschränkung nicht auf eine Vertragsklausel gestützt werden kann, nicht, dass sämtliche Verträge unbesehen öffentlich zu machen seien. Die restlichen Einschränkungsgründe gemäss § 27 IDG müssen selbstverständlich anhand des konkreten Vertrages geprüft werden. So ist insbesondere stets zu prüfen, ob überwiegende Geschäftsgeheimnisse vorliegen könnten.

3] Vorlage 2010-199 an den Landrat vom 11. Mai 2010 zum Gesetz über die Information und den Datenschutz (LRV), S. 36, abrufbar unter https://www.baselland.ch/fileadmin/baselland/files/docs/parl-lk/vorlagen/2010/2010-199.pdf

4] BGÖ, SR 152.3

5] Entscheid des Bundesverwaltungsgerichts vom 7. Dezember 2011, BVGE 2011/52, E.6.3.3

6] Empfehlung des EDÖB vom 27. Februar 2014, E. 24, abrufbar unter http://www.edoeb.admin.ch/oeffentlichkeitsprinzip/00889/01153/index.html?lang=de

7] Tätigkeitsbericht des Datenschutzbeauftragten Basel-Stadt 2012, S. 19, abrufbar unter http://www.dsb.bs.ch/ueber-uns/T%C3%A4tigkeitsberichte.html

III. AUS DEM BERATUNGS-ALLTAG

Die Beratungsaufgabe der ASD gestaltet sich recht unterschiedlich. So gibt es einfache Anfragen, die vom erfahrenen Datenschutzteam rasch beantwortet werden können. Andere Anfragen sind jedoch weitaus komplexer und binden entsprechend mehr Ressourcen.

III.I. AUFZEICHNUNG VON REMOTE SUPPORT SESSIONS

Die ZID hatten Ende 2014 im Zusammenhang mit der geplanten Einführung eines neuen Werkzeugs für den Remote Informatik-Support bei der ASD um Beratung gebeten. Es sei geplant, sämtliche Support Sessions per Video aufzuzeichnen. Die ASD empfahl, keine Videosequenzen der Support Sessions aufzuzeichnen, sondern zunächst die anstehenden Rechtsfragen zu klären und ein Konzept für die Bearbeitung der aufgezeichneten Videosequenzen zu erarbeiten. Ein kritischer Aspekt betraf die Vertraulichkeit der Informationen innerhalb der aufgezeichneten Sequenzen. Je nach Bildschirminhalt konnten diese äusserst vertrauliche Personendaten beinhalten, wie beispielsweise Falldaten bei der Staatsanwaltschaft oder ein Mail zu einem Personaldossier. Die Informationseigner wurden trotz dieser Tatsache nicht ins Projekt einbezogen. Im Rahmen eines Reviews stellte die ASD fest, dass die Aufzeichnung der Support Sessions ohne Wissen der jeweiligen Kunden bereits stattfand und meldete dies umgehend an den zuständigen Informatiksicherheitsbeauftragten. In der Folge wurde festgestellt, dass es für die Videoaufzeichnungen gar keine Notwendigkeit gab. Die Konfiguration der Anwendung wurde daraufhin so abgeändert, dass nunmehr nur Verbindungsdaten (z.B. User-ID der unterstützten Person und Zeitpunkt der Unterstützung), aber keine Videosequenzen mehr aufgezeichnet werden.

III.II. LISTENBEKANNTGABEN AUS EINWOHNERREGISTERN ZU WAHLKAMPFZWECKEN

Im Jahr 2015 standen turnusgemäss Landrats- und National-/Ständeratswahlen an. Viele Parteien wollten im Rahmen dieser Wahlen gewisse Zielgruppen erreichen und auf ihre Programme hinweisen (z.B. alle 18- und 19-Jährigen). Sie gelangten mit der Bitte an die Einwohnerdienste der Gemeinden, ihnen eine Liste mit Personen, die das gewünschte Kriterium erfüllten, auszuhändigen. Die ASD wurde daraufhin mehrfach von Gemeinden angefragt, ob eine Bekanntgabe der Adressdaten aus dem Einwohnerregister trotz der offiziell versandten Wahlpost zulässig sei.

Die ASD konnte den Gemeinden mitteilen, dass dies eine Bekanntgabe zu einem schützenswerten ideellen Zweck – nämlich der Wahrnehmung der demokratischen Rechte – im Sinne von § 3 Abs. 3 des kantonalen Anmeldungs- und Registergesetzes (ARG) darstelle und daher zulässig sei. Die Datenempfänger seien von der Gemeinde allerdings zu verpflichten, die Adressen nur für diesen Zweck zu verwenden und nach Gebrauch zu vernichten.

III.III. BEKANNTGABE VON PERSONENDATEN AN DIE SBB TRANSPORTPOLIZEI DURCH EINE GEMEINDEVERWALTUNG

Die Transportpolizei der SBB hatte von einer Gemeinde neben Angaben zu einem Jugendlichen auch Informationen über dessen Erziehungsberechtigte verlangt. Die Gemeinde wollte von der ASD wissen, ob sie diese weiterführenden Angaben machen dürfe.

Nach kurzen Abklärungen stellte die ASD fest, dass die Transportpolizei diese Angaben zu Handen der Jugendanwaltschaft BL erhob. Die Jugendanwaltschaft benötigte allerdings nur Angaben zur Identität des Jugendlichen, da sie weitergehende Informationen selber in den entsprechenden Systemen abrufen kann. Es gab für die Transportpolizei also keine Notwendigkeit, die Angaben der Erziehungsberechtigten auch noch einzuholen.

III.IV. ZUGANG ZU ABGESCHLOSSENEN STRAFAKTEN IM RAHMEN EINER WISSENSCHAFTLICHEN ARBEIT

Die Jugendanwaltschaft BL hatte eine Anfrage einer auswärtigen Universität erhalten, die im Rahmen einer wissenschaftlichen Arbeit gerne Zugriff auf bestimmte abgeschlossene Strafakten der Jugendanwaltschaft wollte. Die Jugendanwaltschaft wollte nun wissen, unter welchen Umständen dies möglich und was zu beachten sei.

Die ASD konnte der Jugendanwaltschaft BL bestätigen, dass es sich hierbei um eine Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck im Sinne von § 20 des kantonalen IDG handle. Ein solcher Zweck liegt beispielsweise dann vor, wenn die Personendaten für Wissenschaft oder Forschung benötigt werden. Die ASD machte die Jugendanwaltschaft darauf aufmerksam, dass sie die Empfängerin schriftlich verpflichten müsse, die Personendaten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zuliesse, und dass die Auswertungen nur so bekannt gegeben werden dürften, dass keine Rückschlüsse auf die betroffenen Personen möglich seien.

An dieser Stelle sei noch einmal darauf hingewiesen, dass die ASD seit Inkrafttreten des IDG selber keine formelle Prüfung mehr vornimmt, ob die Voraussetzungen für die Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck vorliegen. Diese Prüfung hat nunmehr das zuständige öffentliche Organ vorzunehmen.

III.V. VERSAND VON PENSENLISTEN PER MAIL

Eine Lehrperson meldete der ASD, dass alle Lehrer von der Schulleitung per E-Mail «Pensenlisten» sämtlicher an der Schule tätigen Lehrer zugesandt bekommen hätten. Darauf waren einerseits das Anstellungsverhältnis und der jeweilige Stundenplan der Lehrpersonen ersichtlich. Darüber hinaus enthielten die Listen aber auch Angaben über effektiv erteilte und ausbezahlte Stunden, Vertragsdauer, Lohnfortzahlung und Altersentlastung aller Lehrpersonen. Die Lehrperson wollte wissen, wie diese Bekanntgabe datenschutzrechtlich zu beurteilen sei.

Die ASD stellte fest, dass es für eine derartige Datenbekanntgabe keine gesetzliche Grundlage gab und zudem auch die Notwendigkeit nicht begründet werden konnte. Das Lehrerkollegium muss nicht über die genauen Anstellungsverhältnisse des gesamten Lehrkörpers Bescheid wissen. Die Datenbekanntgabe erfolgte somit klarerweise unrechtmässig.

III.VI. PUBLIKATION VON STUNDENPLÄNEN IM INTERNET

Eine Lehrperson war nicht damit einverstanden, dass ihre Schulleitung die Stundenpläne aller Lehrpersonen frei zugänglich im Internet veröffentlichte, weil so jedermann – allenfalls auch eine Person mit unlauteren Absichten – im Internet erfahren könne, wann sie unterrichte. Die ASD klärte den Sachverhalt ab und stellte fest, dass es keine Notwendigkeit gab, Namen auf den Stundenplänen im weltweiten Netz zu publizieren. Stattdessen empfahl sie die Schaffung eines passwortgeschützten Bereichs auf der Schulwebsite.

III.VII. DETAILLIERTE ANGABEN VON KRANKHEITSKOSTEN AN DIE STEUERVERWALTUNG

Wiederholt wenden sich Steuerpflichtige an die ASD, weil sie beim Abzug von selbstgetragenen Krankheitskosten von der Steuerverwaltung aufgefordert werden, eine detaillierte Aufstellung der Krankheitskosten von ihrer Krankenkasse beizulegen. Auf solchen detaillierten Listen sind unter anderem die Namen von Ärzten, allenfalls deren Fachbereiche, Therapiedetails und bezogene Medikamente aufgeführt. Dadurch kann die Steuerverwaltung durchaus Rückschlüsse auf allfällig vorliegende Krankheiten ziehen.

Die Steuerverwaltung ist gesetzlich ermächtigt, für die Erstellung der Steuerveranlagung und zur Überprüfung von geltend gemachten Abzügen gewisse Daten von den Steuerpflichtigen zu verlangen. Dabei ist sie jedoch immer an das Verhältnismässigkeitsprinzip gebunden, darf also nicht mehr Daten verlangen,

als sie zur Bemessung und zur Prüfung der Abzüge benötigt. Werden hohe Abzüge gemacht oder bestehen Unklarheiten, kann sie im Einzelfall zur Klärung weitere Angaben verlangen. Angaben, die für die Bemessung der Abzüge nicht zwingend erforderlich sind (z.B. Name des behandelnden Arztes, des Medikaments), darf die steuerpflichtige Person in der detaillierten Auflistung der Krankheitskosten abdecken bzw. schwärzen, bevor sie sie der Steuerverwaltung zustellt.

III.VIII. ERFASSUNG DER AUTONUMMER IM RAHMEN DER PARKRAUM-BEWIRTSCHAFTUNG

Eine Gemeinde stellte im Rahmen einer neuen Parkraumbewirtschaftung Parkuhren auf, welche zur Begleichung der Parkgebühr die Eingabe der Autonummer verlangen. Eine Privatperson wollte von der ASD wissen, ob dies zulässig sei. Sie befürchtete, dass diese Daten dazu benutzt würden, ihre Bewegungen mit dem Fahrzeug nachzuverfolgen.

Die ASD konnte der Privatperson mitteilen, dass die Gemeinde die Daten unmittelbar nach Ablauf der Parkzeit löscht und keine weitergehende Nutzung der erfassten Autonummern erfolgt. Der vom Bürger befürchtete Datenmissbrauch lag also nicht vor.

III.IX. EINTRAG VON VERTRAULICHEN INFORMATIONEN IM OUTLOOK-KALENDER DER VORGESETZTEN PERSON

Eine beim Kanton angestellte Person hatte arbeitsrechtliche Schwierigkeiten mit ihrer vorgesetzten Person. Sie entdeckte in deren Outlook-Kalender einen Besprechungstermin, dem eine E-Mail der Personalabteilung mit vertraulichen Daten über sie angehängt war. Sämtliche Mitarbeitende des Teams hatten ebenfalls die Möglichkeit, den Eintrag inkl. des angehängten E-Mails mit den vertraulichen Informationen zu lesen. Die ASD bestätigte der betroffenen Person, dass Vertrauliches im Outlook-Kalender immer als «Privat» zu markieren sei. Diese Vorgabe ist im Benutzungsreglement Informatikmittel des Kantons ausdrücklich festgehalten und von sämtlichen angestellten Personen des Kantons entsprechend zu handhaben. Die ASD hat bereits in den vergangenen Jahren mehrfach darauf hingewiesen, dass es wegen der mangelhaften Umsetzung dieser Vorgaben regelmässig zu Verstössen gegen das Datenschutzgesetz und zu Verletzungen des Amtsgeheimnisses kommt.

IV. KONTROLL-TÄTIGKEIT

Die Aufsichtsstelle Datenschutz pflegt eine rollende, risikobasierte Kontrollplanung, welche in anlassfreie Kontrollen mündet. Daneben werden sogenannte anlassbedingte Kontrollen durchgeführt.

IV.I. WENN DER «DRUCKER» ALLES WEISS

Die meisten neueren «Drucker» sind heute multifunktional und können viel. Neben drucken können sie meist auch faxen, scannen und kopieren. Diese Geräte besitzen beachtliche Rechen- und Speicherkapazitäten, sind kommunikationsfähig und können sogar aus der Ferne gesteuert werden. Zudem führen sie ein ausführliches Protokoll. Aus diesen Eigenschaften in Verbindung mit der Tatsache, dass mit den Geräten alle möglichen Arten von (Personen-) Daten gespeichert und ausgedruckt werden, ergeben sich Risiken für die Informationssicherheit und den Datenschutz.

Bei ihrer Kontrolle stellte die ASD verschiedene offene Punkte fest. Eine zentrale Feststellung war dabei, dass die Beschaffung der Geräte seitens des Kantons ausschliesslich durch die Schul- und Büromaterialverwaltung durchgeführt wird und die Dienststellen als Informationseigner, welche die Geräte nutzen, nicht in den Beschaffungsprozess einbezogen worden waren. Die Informationseigner kannten die Konfigurationsmöglichkeiten der von ihnen verwendeten Geräte nicht und waren somit nicht in der Lage, die auf vielen Geräten vorhandene Einstellung «sicheres Löschen nach dem Druck» zu wählen. Weitere Feststellungen betrafen die sichere Entsorgung der Festspeicher sowie die fehlende Schulung der Mitarbeitenden bzgl. Vertraulichkeit beim Umgang mit den Geräten.

Bevor diese Mängel behoben werden können, müssen die involvierten Behörden in einem ersten Schritt die Verantwortlichkeiten bei Beschaffung, Konfiguration, Installation und Entsorgung dieser Geräte klären. Die ASD wird den weiteren Verlauf dieses Geschäfts aufmerksam beobachten und wenn nötig intervenieren.

IV.II. PERSONALDOSSIERS 2.0 (ELEKTRONISCHES PERSONALDOSSIER)

Die Personaldossiers der Kantonsangestellten werden mit einem SAP-Modul (SAP HCM) elektronisch geführt. Bei der elektronischen Bearbeitung der teils sensitiven Daten stellen sich Fragen zur Informationssicherheit und zu den damit verbundenen organisatorischen und technischen Massnahmen zum Schutz der Ressourcen. Die ASD beschloss deshalb bereits 2014, diesen Bereich in die risikobasierte Kontrollplanung aufzunehmen und ein spezialisiertes Unternehmen mit dem technischen Audit der SAP-HCM-Umgebung zu beauftragen, da die Aufsichtsstelle aus wirtschaftlichen Gründen kein vertieftes Know-how über alle Systeme à jour halten kann.

Die Kontrolle ergab, dass sich das Personalamt stark an den personalrechtlichen Vorgaben orientiert, jedoch gewisse datenschutzrechtliche Vorgaben sowie Vorgaben und «good practices» zur Informationssicherheit oft nicht angemessen erfüllte. Konkret zeigte sich Handlungsbedarf beim Benutzerberechtigungs- und Rollenkonzept, welches die Anforderungen an die Verhältnismässigkeit nicht vollumfänglich erfüllt. Die ASD erkannte zudem Handlungsbedarf hinsichtlich der Nutzung administrativer Passwörter und des administrativen sowie technischen Benutzermanagements. Insbesondere müssen auch die Abstimmung sowie die Effektivität der Zusammenarbeit mit dem zentralen externen Partner optimiert werden. Die Kontrolle identifizierte ausserdem mehrere Schwachstellen im Bereich der physischen Sicherheit. Die kontrollierte Behörde wird die ASD im nächsten Jahr gemeinsam mit den involvierten Leistungserbringern über die getroffenen Massnahmen informieren.

IV.III. DATENSCHUTZ IN EINEM ALTERS- UND PFLEGEHEIM

Die Gemeinden sind verpflichtet, für eine ausreichende stationäre Betreuungs- und Pflegestruktur ihrer Einwohnerinnen und Einwohner im Alter zu sorgen. Sie können private gemeinnützige Institutionen damit betrauen. Aufgrund der Sensitivität der in Pflegeinstitutionen bearbeiteten Personendaten startete die ASD Ende 2014 gemeinsam mit externen Experten eine Kontrolle in einem Alters- und Pflegeheim. Im Fokus der Kontrolle standen das elektronische Abklärungssystem BESA, mit dem unter anderem die Pflegestufe ermittelt wird, sowie die elektronische Pflegedokumentation easyDOK.

Die Kontrolle ergab, dass die datenschutzrechtlichen Vorgaben grundsätzlich gut erfüllt werden. Handlungsbedarf identifizierte die Kontrolle u.a. im Bereich des Passwort- und Benutzermanagements, der Aufzeichnung und Aufbewahrung von Betriebssystem-Logdateien und Datenbank-Protokollen sowie bei der ungesicherten Übermittlung von Personendaten über das Anmeldeformular.

IV.IV. BYOD: VERTRAUEN DANK DATENSCHUTZ

Verschiedene Benutzer aus Dienststellen mit besonderem Bewusstsein für den Umgang mit vertraulichen Informationen hatten sich geweigert, ihre selbst gekauften Smartphones im Sinne von Bring your own device (BYOD) in die Mobile Device Management Anwendung (MDM) des Kantons einbinden zu lassen. Grund dafür war, dass diese Benutzer eine zu weitgehende Überwachung durch den Arbeitgeber befürchteten. Die ASD führte daraufhin eine anlassbedingte Kontrolle der MDM-Konfiguration durch und stellte einige Mängel fest. Die ASD verlangte, dass die Datenbearbeitungen im MDM datenschutzkonform durchgeführt werden. Die Konfiguration der MDM-Anwendung wurde daraufhin geändert (u.a. wurde auf die Aufzeichnung von Ortungsinformationen verzichtet), und die Benutzer wurden in einem Merkblatt darüber informiert, welche Daten über sie und ihre Nutzung im MDM gespeichert werden. Durch ihre Vermittlung hat die ASD dazu beigetragen, dass das Vertrauen der Benutzer in die MDM-Anwendung wiederhergestellt wurde. Aufgrund des wiedergewon-

nenen Vertrauens haben sich auch diejenigen Mitarbeitenden zur Einbindung ihrer Geräte in MDM entschieden, welche sich ursprünglich geweigert hatten, ihre eigenen Geräte dafür zur Verfügung zu stellen. Auf diese Weise wurde verhindert, dass der Kanton für diese Mitarbeitenden rund siebzig Smartphones extra beschaffen musste.

IV.V. DAS ZENTRALE PERSONENREGISTER ARBO: EIN BAUM MIT VIELEN WURZELN UND ÄSTEN

Seit dem 1. Januar 2008 bestimmt das Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (SR 431.02, RHG), welche Angaben die Kantone in ihren Einwohnerregistern führen müssen. Bei der Umsetzung dieses Gesetzes hatte der Kanton Basel-Landschaft entschieden, ein zentrales kantonales Personenregister zu schaffen. Den grössten Teil dieses kantonalen Personenregisters «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 zu den juristischen Personen mit Grundeigentum im Kanton Basel-Landschaft.

In den letzten Jahren ist arbo wie geplant zu einem Kernelement des kantonalen Personendatenaustauschs geworden; die Personendaten aus arbo werden rege abgefragt und ausgetauscht. 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 des Berichtsjahres im Detail geplant und begonnen. Die Kontrolle vor Ort wurde auf Anfang 2016 terminiert, und der Bericht wird im ersten Halbjahr 2016 erwartet.

IV.VI. KLINIKINFORMATIONSSYSTEM ALS INFORMATIONSDREHSCHEIBE IM SPITALWESEN

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 entschieden, eine Kontrolle von Teilbereichen des Klinikinformationssystems des Kantonsspitals am Standort Liestal durchzuführen.

Bei der Kontaktaufnahme wurde die ASD gebeten, mit der Kontrolle so lange zuzuwarten, bis die nächsten Projekte abgeschlossen sind. Diese Bitte wird oft geäussert. Allerdings wird im Informatikumfeld ohnehin selten ein Zustand erreicht, in dem es keine aktiven Projekte gibt. Die ASD beschloss deshalb, das Prüfgebiet möglichst für die anstehenden Projekte nutzbar zu definieren und im Hinblick auf das KIS-Konsolidierungsprojekt das Augenmerk der Kontrolle schwerpunktmässig auf die Prozesse zu legen. Die technische Prüfung sollte sich auf die grundlegenden Informationssicherheitsaspekte konzentrieren. Diese datenschutzrechtliche Kontrolle wurde Ende des Berichtsjahres im Detail geplant und begonnen. Die Kontrolle vor Ort und der Schlussbericht zur Kontrolle folgen Anfangs 2016.

V. STELLUNGNAHMEN

Die ASD hat sich im Berichtsjahr aus datenschutzrechtlicher Sicht u.a. zu folgenden Themen geäussert: Internes Kontrollsystem IKS, Gesetz über die Sozial-, die Jugend- und Behindertenhilfe, e-Recruiting, Personensicherheitsprüfung, Prämienverbilligung in der Krankenpflegeversicherung, Schuladministrationslösung (SAL), Datenschutzrichtlinie der Spitex, Leistungsvereinbarung Schulsozialdienst, Gesetz über die Behindertenhilfe, Vergaberecht, e-Government Strategie Schweiz, e-Public, Anmelde- und Registergesetz, Mobile Device Management, Herausgabe von Patientendossiers, Anschluss an das Personenregister (arbo), Einführungsgesetz zur StPO, Informationssicherheits- und Datenschutzkonzepte diverser Behörden, Sozialhilfeverordnung, Asylverord-

nung, Verschlüsselung sensitiver Daten, Verordnung über den Umgang mit Personaldaten, Informationsaustausch im Rahmen von Lean Management sowie Leistungsvereinbarungen mit unterschiedlichen Institutionen.

Die Themenvielfalt war herausfordernd und spannend zugleich. Wie in jedem Jahr fehlten zuweilen die gesetzlichen Grundlagen für die Vorhaben der kantonalen Verwaltung. Die ASD musste erneut darauf hinweisen, dass jedes staatliche Handeln durch ein Gesetz abgestützt sein muss. Ebenso regelmässig stellte die ASD fest, dass im Rahmen von Leistungsvereinbarungen mit Dritten die Kontrollrechte des Kantons nicht geregelt wurden.

VI. ÖFFENTLICHKEITSARBEIT

VI.I. VORTRAG AM SICHERHEITSTAG DES KANTONS ZU «BIG DATA»

Rund 260 Mitarbeitende der Verwaltung konnten sich am Sicherheitstag 2015 über die Themen «Gefahren am Arbeitsplatz, «Internet der Dinge» sowie «Big Data» informieren und wertvolle Impulse für ihre tägliche Arbeit aber auch für ihr Privatleben mitnehmen.

Die Datenschutzbeauftragte wurde von den Organisatoren eingeladen über Chancen und Risiken von «Big Data» zu sprechen. Sie zeigte anhand von Anwendungsbeispielen aus der Medizin und aus der Sicherheits- und Polizeiarbeit, wie heute grosse Datenmengen aus vielfältigen Quellen gesammelt, aufbereitet und für bestimmte oder unbestimmte Zeit für Analysen verfügbar gemacht werden können. Ferner erläuterte sie bestehende Risiken von Big Data am Beispiel von «Personalized Pricing», «Kreditprüfungen» und «Backgroundchecks von Stellensuchenden». Der Sicherheitstag des Kantons bildete einmal mehr einen wertvollen Beitrag für die Sensibilisierung der Mitarbeitenden.

VI.II. SCHULUNGEN

Der gesetzliche Auftrag der ASD umfasst auch die Beratung öffentlicher Organe (§ 40 Abs. 1 Bst. c IDG). Eine Form der Beratung bilden seit jeher Schulungen. Anlässlich einer Schulung können einerseits die Grundsätze des Datenschutzes – und auch des Öffentlichkeitsprinzips – vermittelt werden, andererseits auch anhand der sich für die jeweiligen Teilnehmer stellenden Fragen aus der Praxis konkretisiert werden.

Auch 2015 führte die ASD wieder verschiedene Schulungen durch. Wie jedes Jahr wirkten wir bei der Schulung der Auszubildenden des Kantons im Rahmen der überbetrieblichen Kurse (üK) mit. Ein weiterer Stammgast war die Klasse der Polizeiaspirantinnen und Polizeiaspiranten, die in ihrer Tätigkeit zuhauf mit besonders heiklen Daten zu tun haben. Ferner wurden wir von der FHNW im Rahmen des CAS öffentliche Verwaltung eingeladen, das Thema Datenschutz zu schulen sowie den entsprechenden Prüfungsteil zu gestalten. Auf Anfrage des KIGA führte die ASD zudem eine fachspezifische Schulung durch, anlässlich welcher die verschiedenen praktischen Probleme, die sich in diesem Bereich besonders im Austausch mit anderen Behörden ergeben, erörtert wurden.

Leider ergab es sich aufgrund der geringen Zahl von Anmeldungen auch im Berichtsjahr nicht, dass die vom Personalamt jährlich angesetzten Kurse zu Datenschutz und Öffentlichkeitsprinzip durchgeführt werden konnten. Angesichts der zunehmenden Digitalisierung und der damit verbundenen vielfältigen rechtlichen, technischen aber auch gesellschaftlichen Fragestellungen erstaunt es, dass das Interesse am Thema – ausserhalb von Expertenkreisen – offenbar wenig vorhanden ist.

Im Verlauf der Schulungen ist es der ASD stets ein Anliegen, dass den beteiligten Personen das auf den ersten Blick etwas theoretisch-rechtlich anmutende Gebiet des Datenschutzes in praktischer Sicht nähergebracht wird. Schliesslich sind die Mitarbeitenden des Kantons und der Gemeinden zwar untertags selber Datenbearbeiter, aber eben auch stets und immer intensiver selber Gegenstand von Datenbearbeitungen. Eine Sensibilisierung für dieses Thema bietet demnach nicht nur einen Mehrwert für die tägliche Arbeit, sondern auch in persönlicher Hinsicht.

VII. KANTONALE, NATIONALE UND INTERNATIONALE ZUSAMMENARBEIT

VII.I. ZUSAMMENARBEIT MIT DEN SICHERHEITSBEAUFTRAGTEN IM KANTON UND MIT DER ZENTRALEN INFORMATIK

Im Berichtsjahr hat sich der Kontakt mit den für die Informationssicherheit zuständigen Personen im Kanton intensiviert. Im Rahmen der Awareness-Kampagne zur Vorabkontrolle und der seitens der Direktionen geplanten Einführung von Hermes 5.1 hat die ASD eine Arbeitsgruppe aus Sicherheitsbeauftragten des Kantons intensiv dabei unterstützt, die Dokumentvorlagen «Schutzbedarfsanalyse», «ISDS-Konzept» und «Grundschutz» auf die Situation im Kanton anzupassen. Ebenfalls lieferte die ASD u.a. auf der Basis von Feststellungen ihrer Kontrolltätigkeit Hinweise zur Überarbeitung des Informationssicherheitskonzeptes ISK.

Die ASD unterstützte im Berichtsjahr die IPK bei der Ausbildung der Informatiksicherheitsbeauftragten und eines Teils der Projektleiter in der Projektführungsmethode HERMES. Diese Ausbildung war auch aus Sicht des Datenschutzes sehr nützlich, da die enge Verzahnung der Vorabkontrolle mit HERMES den Aufwand der Projektleitenden und der Aufsichtsstelle minimiert und gleichzeitig die Qualität der Projekte in Sachen Datenschutz und Informationssicherheit erhöht. Seit dem Antritt des neuen ZI-Leiters kann eine deutliche Gewichtsverlagerung zu strukturiertem Projektvorgehen festgestellt werden, was letztlich auch die Arbeit der ASD erleichtern wird.

Die Aufsichtsstelle Datenschutz trifft sich in regelmässigen Abständen mit dem Leiter ZI und dem Leiter der IPK. Dieser Austausch dient dem rechtzeitigen Erkennen von Handlungsbedarf auf beiden Seiten, mit dem Ziel, die Aspekte des Datenschutzes und der Informationssicherheit im Kanton möglichst effizient zu bearbeiten.

VII.II. FINANZKONTROLLE

Die Revisionsleitung Informationssicherheit und Datenschutz hat auch im 2015 den Kontakt mit den Revisoren der Finanzkontrolle gesucht und sie zu den erfolgten und geplanten Kontrollen informiert. Die Aufsichtsstelle Datenschutz versucht so, Synergien zu nutzen und zu vermeiden, dass bei einer Behörde zwei Kontrollen im selben Jahr durchgeführt werden.

VII.III. PRIVATIM

Die Vereinigung der schweizerischen Datenschutzbehörden (privatim) führte auch 2015 wieder zwei Plenumsveranstaltungen durch. Die Frühjahrstagung wurde von der Datenschutzbeauftragten des Kantons Aargau organisiert und beschäftigte sich mit den Themen «Open Government Data» sowie mit Fragen des Öffentlichkeitsprinzips. An der Herbsttagung in Luzern beschäftigten sich die Datenschutzbeauftragten mit der Kontrolle der Staatsschutztätigkeit durch kantonale Datenschutzbehörden. Die ASD war an beiden Veranstaltungen vertreten.

VII.IV. SCHENGEN-KOORDINATIONSGRUPPE

Im Berichtsjahr nahm die ASD an zwei Sitzungen der «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengener Assoziierungs-Abkommens» teil. Zu den ständigen Traktanden dieser Gruppe gehören die Information über die aktuellen Entwicklungen im europäischen Datenschutzrecht sowie die Berichterstattung über schengenrelevante Kontrollen in Bund und Kantonen. Im Berichtsjahr hatten die Datenschutzbeauftragten zudem die Möglichkeit fedpol zu besuchen.

VII.V. ARBEITSGRUPPE INFORMATION AND COMMUNICATION TECHNOLOGY (AG ICT)

In der AG ICT vernetzen sich die Informatikerinnen und Informatiker der schweizerischen Datenschutzbehörden. Im Berichtsjahr hat die AG ICT eine Übersicht über die Publikationen der schwei-

zerischen Datenschutzbehörden erstellt. Ausserdem wurde das Merkblatt «Datenschutztechnische Anforderungen an Klinikinformationssysteme» überarbeitet. Ebenso wurden verschiedene Merkblätter zur gemeinsamen Nutzung durch die Datenschutzbehörden erstellt. Die ASD nutzt die Kontakte in der AG ICT ausserhalb der periodischen Sitzungen bei der Behandlung von Sachgeschäften, die potenziell bei anderen Kantonen relevant sein könnten bzw. waren.

VIII. AUSBLICK

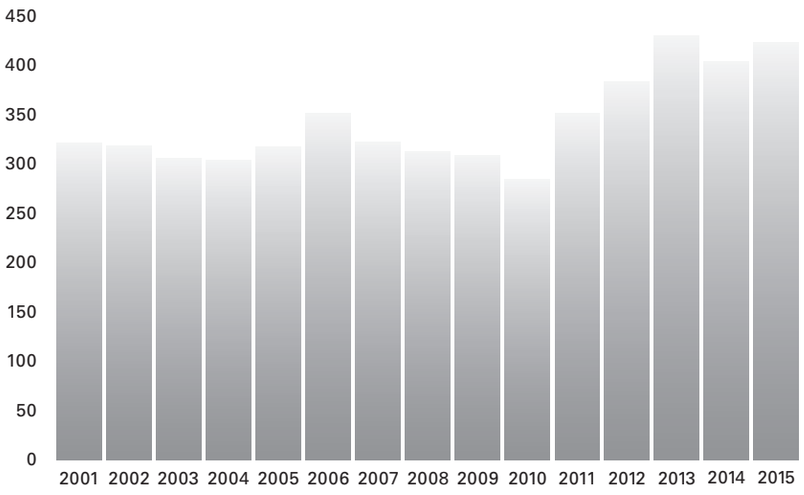
Datenerfassung, Datenweitergabe und Datenanalyse werden durch die Digitaltechnik immer einfacher. Gleichzeitig steigen die Anforderungen an die Informationssicherheit und an den Schutz der Privatsphäre.

Der Staat muss sich immer wieder die Frage stellen, wie er die Privatsphäre der Bürgerinnen und Bürger angesichts der anhaltenden technologischen Entwicklungen schützen kann. Diese Frage wird aufgrund der zunehmenden Vernetzung von Datenbanken, des Auslagerns ganzer Datenbestände in eine Cloud, des Auswertens grosser Datenbestände mittels Big Data, Mobile Computing etc. immer komplexer. Die ASD verfügt über Fachwissen, das sie gerne weitergibt. Sie wird die Verantwortlichen deshalb im Rahmen von Vorabkontrollen und Stellungnahmen auf rechtliche, technische und organisatorische Risiken geplanter Datenbearbeitungsprozesse hinweisen und sie – soweit es ihre Mittel erlauben – bei der Problemlösung unterstützen. Diesen präventiven Ansatz wird die ASD auch in Zukunft prioritär verfolgen. Ergänzend wird sie weiterhin ihren Kontrollauftrag wahrnehmen.

Im Weiteren wird sich die ASD mit einer Verzichtsplanung und einer Reorganisation beschäftigen müssen, da die vom Landrat beschlossene Mittelkürzung von 22% nicht ohne Folgen bleiben wird. Die Mittelkürzung ohne Änderung des gesetzlichen Auftrags wird dazu führen, dass die ASD nicht mehr alle Aufgaben innert nützlicher Frist erledigen kann. Behörden, die eine zeitnahe Beratung möchten, werden daher vermehrt auf ihre eigenen Ressourcen (IT-Sicherheitsexperten, Rechtskonsulenten, Rechtsdienste etc.) zurückgreifen müssen. Die Datenschutzbeauftragte bedauert diese Entwicklung, sie hat sie aber nicht zu verantworten.

ANHANG

GESCHÄFTE



ART DER GESCHÄFTE