AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

TÄTIGKEITSBERICHT 2017

2018/040-09

AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragter:	Markus Brönnimann
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 der Datenschutzbeauftragte dem Landrat Bericht über seine Tätigkeit sowie über wichtige Feststellungen und Beurteilungen.

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

INHALTSVERZEICHNIS

Vorwort	**3**
Aktuell	**3**
Aus dem Beratungsalltag	**4**
Vorabkontrolle	**11**
Kontrolltätigkeit	**13**
Öffentlichkeitsprinzip	**14**
Anhang	**16**

VORWORT

Zum Ende dieses Berichtjahres verliert die Aufsichtsstelle Datenschutz (ASD) Ursula Stucki nach rund 17-jähriger Tätigkeit als Datenschutzbeauftragte des Kantons Basel-Landschaft. Sie geht vorzeitig in Pension. Ursula Stucki ist eine in der Datenschutzszene schweizweit bekannte und etablierte Persönlichkeit mit viel Erfahrung und einem grossen Wissen. Sie hat während ihrer Tätigkeit einen bedeutenden Beitrag dazu geleistet, dass der Datenschutz und der sichere Umgang mit Informationen in unserem Kanton kontinuierlich verbessert worden sind. Während ihrer gesamten Amtszeit hat sie sich mit grossem Einsatz beharrlich und erfolgreich für den Schutz der Privatsphäre der Bürgerinnen und Bürger eingesetzt. Sie hat bereits früh erkannt, dass sie im Zuge der fortschreitenden Digitalisierung IT-Wissen innerhalb der ASD aufbauen musste. Sie gehört damit zu den Pionierinnen unter den Datenschutzbeauftragten in der Schweiz. Die Zusammenhänge zwischen Recht und IT und die enge Zusammenarbeit zwischen diesen Bereichen sind die Basis, auf der die ASD sich auch künftig Herausforderungen kompetent stellen kann.

Nach seiner Wahl durch den Landrat im November 2017 zum neuen Datenschutzbeauftragten hat Markus Brönnimann per April 2018 die Nachfolge von Ursula Stucki angetreten. Er durfte ein engagiertes Team mit kompetenten Mitarbeitenden übernehmen. Wie in der Vergangenheit wird auch künftig eines der Ziele des ASD-Teams sein, mit dem jeweiligen Gegenüber eine gesetzeskonforme, praktikable Lösung im Interesse eines optimalen Datenschutzes zu finden.

AKTUELL

DAS INFORMATIONS- UND DATENSCHUTZGESETZ (IDG) UND DIE ENTWICKLUNG AUF DER EUROPÄISCHEN EBENE

Das Thema Datenschutz erlebte in der medialen Berichterstattung im Berichtsjahr (und noch stärker 2018) eine echte Renaissance. Neben diversen Vorfällen im Berichtsjahr – wie beispielsweise die 800'000 entwendeten Swisscom-Kundendaten – war der hauptsächliche Grund dafür, dass per 25. Mai 2018 die Regeln der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) ihre Wirkung entfalten. Ihre Bedeutung für die Schweiz im Allgemeinen und unseren Kanton im Besonderen wurde bereits in den beiden vorherigen Tätigkeitsberichten skizziert. An dieser Stelle deshalb nur eine kurze Zusammenfassung.

Die DSGVO regelt die Bearbeitung von Personendaten innerhalb der EU. Sie enthält aber auch eine Bestimmung, welche den Anwendungsbereich auf öffentliche Organe und Private ausdehnt, die von ausserhalb der EU Waren oder Dienstleistungen in die EU anbieten. Auf diese Weise soll vermieden werden, dass Unternehmen ihren Sitz ausserhalb der EU ansiedeln und sich unter Umgehung europäischer Gesetze einen Wettbewerbsvorteil sichern. Für die Anwendbarkeit der DSGVO müssen allerdings klare Anzeichen vorhanden sein, dass das fragliche Angebot (auch) in den EU-Raum ausgerichtet ist. Die reine Erreichbarkeit einer Website reicht zum Beispiel nicht aus. Auch wenn ein Unternehmen oder ein öffentliches Organ einen oder mehrere Arbeitnehmende mit Wohnsitz in der EU beschäftigt, begründet das noch keine Anwendbarkeit der Verordnung.

Die rechtliche Unsicherheit rund um die DSGVO ist derzeit noch gross. Es wird an den Gerichten liegen, über die Auslegung der Bestimmungen Klarheit zu schaffen. Für den Kanton und die Gemeinden geht die ASD derzeit davon aus, dass die DSGVO abgesehen von ganz wenigen möglichen Ausnahmen keine direkte Wirkung entfalten wird.

Dies bedeutet jedoch nicht, dass die neuen europäischen Gesetze zum Datenschutz ganz spurlos am Kanton vorbei gehen werden. Denn neben der DSGVO sind zwei neue bzw. revidierte Erlasse von direkter Bedeutung für die Schweiz, da sie über Staatsverträge eingebunden ist. Da ist einerseits die Richtlinie der EU für die Datenbearbeitung im Rahmen der Verfolgung von Straftaten, andererseits die Revision der Datenschutzkonvention des Europarates. Beide

Regelungen sind nicht direkt anwendbar und müssen somit ins nationale Recht überschrieben werden. Die Richtlinie gehört zum sogenannten Schengen-Besitzstand, und die Schweiz hat bereits beschlossen, sie umzusetzen. Die Schweiz wird auch die Europaratskonvention ratifizieren. Deshalb wird auch im Kanton Basel-Landschaft gegenwärtig das IDG revidiert, um die Änderungen, die sich aus den erwähnten Erlassen ergeben, nachzuvollziehen.

Das zeitliche Zusammentreffen aller europäischen Erlasse zum Thema Datenschutz ist nicht zufällig, sie sind auch inhaltlich zu einem grossen Teil aufeinander abgestimmt.

AUS DEM BERATUNGS-ALLTAG

BEKANNTGABE DER ADRESSEN VON NEUELTERN AN EIN PRIVATWIRTSCHAFTLICHES UNTERNEHMEN

Ein privates Unternehmen stellte bei einer Gemeinde den Antrag auf Herausgabe von Geburtsadressen. Die Adressen sollten für eine Werbeaktion verwendet werden. Die Aktion sah vor, dass Hostessen die Neueltern besuchen, ihnen Tipps und Ratschläge geben, auf Geschäfte in unmittelbarer Nähe aufmerksam machen sowie Gutscheine von Geschäften aus der Wohnregion und Geschenkkoffer überreichen. Die Gemeinde stellte der ASD die Frage, ob sie dem Unternehmen die Adressen herausgeben dürfe.

Damit eine Gemeinde Daten über mehrere Personen, die nach Merkmalen (wie hier die Geburten) geordnet sind, an die gesuchstellende Person herausgeben darf, muss diese gemäss § 3 Abs. 3 des kantonalen Anmeldungs- und Registergesetzes (ARG) die Daten für schützenswerte ideelle Zwecke verwenden wollen. Die ASD stellte in diesem Fall fest, dass das Unternehmen mit der Aktion die Gewinnung von Neukunden und damit einen wirtschaftlichen Zweck verfolgte. Ein schützenswerter ideeller Zweck lag somit nicht vor. Die Voraussetzungen von § 3 Abs. 3 ARG waren entsprechend nicht erfüllt und eine Bekanntgabe der Adressen nicht erlaubt.

BEKANNTGABE DES STROMVERBRAUCHS EINER LIEGENSCHAFT BZW. DER ADRESSE AN DIE POLIZEI BL

Die ASD wurde von der Elektra Baselland (EBL) angefragt, ob sie der Polizei BL den Stromverbrauch einer bestimmten Liegenschaft bzw. die Adresse bekanntgeben dürfe – oder ob dafür eine amtliche Verfügung nötig sei.

Die ASD ist bei der Polizei BL vorstellig geworden, um den Sachverhalt genauer abzuklären. Die Polizei BL bestätigte der ASD, dass sie einem Hinweis nachgegangen war, wonach in der Liegenschaft möglicherweise eine Hanf-Indooranlage betrieben würde. Im Rahmen der polizeilichen Vorermittlung wollte die Polizei BL deshalb von der EBL wissen, ob der Stromverbrauch in der Liegenschaft auffällig sei (erhöhter, nicht der Norm entsprechender Stromverbrauch). Sollte sich der Verdacht bestätigen, wollte die Polizei BL bei der Staatsanwaltschaft BL Antrag auf Verfahrenseröffnung einreichen und eine Stromedition auf die bezeichnete Liegenschaft bei der EBL beantragen, damit die Erkenntnisse in die Verfahrensakten hätten übernommen werden können.

Die Polizei BL konnte sich bei ihren Ermittlungen auf eine gesetzliche Grundlage stützen (§ 3 Abs. 1 lit. b des kantonalen Polizeigesetzes (PolG, SGS 700) sowie Art. 299, 300 und 306 der bundesrechtlichen Strafprozessordnung (StPO, SR 312)). Danach dürfen der Polizei BL im Einzelfall und auf konkrete Anfrage hin Auskünfte über einen auffälligen Stromverbrauch einer Liegenschaft erteilt werden. Erst in einem zweiten Schritt und nur bei Vorliegen eines entsprechenden Befehls der Staatsanwaltschaft müssten darüber hinaus auch konkrete Unterlagen etc. herausgeben werden.

BEKANNTGABE VON SCHÜLERADRESSEN AN GEMEINDERAT

Um abzuklären, ob in einer Gemeinde ein Schulbus Sinn machen könnte, wollte der Gemeinderat von den Einwohnerdiensten einer Gemeinde die Adressen aller Schülerinnen und Schüler erhalten. Auf dieser Basis wollte die Exekutive die Schulweglängen berechnen.

Die Adressen von Schülerinnen und Schülern stellen Personendaten gemäss § 3 Abs. 3 IDG dar. Damit öffentliche Organe wie der Gemeinderat Personendaten bearbeiten dürfen, braucht es gemäss § 9 Abs. 1 IDG entweder eine gesetzliche Grundlage oder die Daten müssen zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Die Daten von Schülerinnen und Schülern dürfen gemäss Bildungsgesetz des Kantons Basel-Landschaft nur für schulische Zwecke verwendet werden. Der Gemeinderat konnte sich somit für sein Anliegen auf keine gesetzliche Grundlage stützen.

Die ASD hat als nächstes geprüft, ob die Einwohnerdienste die Daten allenfalls zu nicht personenbezogenen Zwecken gemäss § 20 IDG bekanntgeben könnten, da der Gemeinderat primär an der Schulweglänge und nicht an Informationen zu einzelnen Schülerinnen und Schülern interessiert war. Die ASD bejahte diese Möglichkeit unter der Voraussetzung, dass die Daten soweit und sobald als möglich anonymisiert würden. Da die Adressen (ohne Namen) im Einzelfall womöglich Rückschlüsse auf einzelne Personen zugelassen hätten, müsste, um dem aus dem Verhältnismässigkeitsprinzip fliessenden Grundsatz der Erforderlichkeit nachzukommen, auch die Option geprüft werden, ob anstelle der Wohnadresse die nächstgelegene Bushaltestelle bekanntgegeben werden könnte. In diesem Falle wären keine Personendaten betroffen.

ZUGRIFF DER HEIMLEITUNG AUF ADRESSDATEN EINER KOMMUNALEN FACHSTELLE

Die Leitung eines Alters- und Pflegeheims (APH) wollte von der kommunalen Fachstelle für Altersfragen Adressdaten der Bewohnerinnen und Bewohner, um auf ein Angebot aufmerksam machen zu können. Die Fachstelle verweigerte die Herausgabe aus Datenschutzgründen. Da sich die Daten des anfragenden APH auf demselben Netzwerk befanden wie jene der Fachstelle, verschaffte sich die leitende Person des APH, welche als Administratorin des APH Zugriff auf die Daten von beiden Stellen hatte, die Adressdaten selbst.

Die ASD stellte fest, dass die Fachstelle die Herausgabe der Adressdaten zu Recht verweigert hatte. Für eine Herausgabe bestand keine gesetzliche Grundlage. Ebenso wenig bestand eine solche für das aktive Beschaffen der Daten. Die ASD wies darüber hinaus darauf hin, dass § 8 IDG nicht eingehalten worden war: Danach muss ein öffentliches Organ Informationen durch angemessene organisatorische und technische Massnahmen u.a. vor unrechtmässiger Bearbeitung und Kenntnisnahme schützen. Die betreffende Person hätte gar nicht im Besitz der Administratorrechte sein dürfen.

Die ASD möchte an dieser Stelle einmal mehr darauf hinweisen, dass sich jedes öffentliche Organ stets überlegen muss, welche Person welche Berechtigungen zur Aufgabenerfüllung tatsächlich benötigt, und die Zugriffsrechte entsprechend vergeben muss. Damit wird einerseits das Verhältnismässigkeitsprinzip eingehalten. Andererseits wird ein Zugriff durch Unbefugte verhindert.

ZUTRITT ZU EINER WOHNUNG ZUR ÜBERPRÜFUNG, OB EINE BEI DER GEMEINDE ANGEMELDETE PERSON TATSÄCHLICH DORT WOHNT

Eine Gemeindeverwaltung hatte den Verdacht, dass eine Person womöglich nicht mehr an der gemeldeten Adresse wohnhaft sein könnte. Um zu überprüfen, ob die Person wirklich noch an der gemeldeten Adresse wohnte, wollte die Gemeindeverwaltung der Person einen Besuch abstatten und fragte die ASD an, ob sie dies tun dürfe.

Die ASD gab der Gemeindeverwaltung folgende Auskunft: An- und Abmeldungen in einer Gemeinde sind eine Bringschuld der Bürgerinnen und Bürger. Wird dieser Pflicht nicht nachgekommen, hat die Gemeinde gemäss § 6 des Anmeldungs- und Registergesetzes (ARG) die Möglichkeit, eine Abmeldung von Amtes wegen zu verfügen. Ein Besuch bei der betreffenden Person ist deshalb weder notwendig noch hätte er einen gesetzlichen Rechtfertigungsgrund.

BEKANNTGABE DES NAMENS EINES GESUCHSTELLERS

Gemäss Öffentlichkeitsprinzip (§ 56 der Kantonsverfassung) sind die öffentlichen Organe des Kantons und der Gemeinden dazu verpflichtet, über Angelegenheiten von allgemeinem Interesse aktiv zu informieren sowie auf Gesuche hin Informationen herauszugeben. Die Ausführungsbestimmungen sind im IDG geregelt. Sind bei einem Zugangsgesuch um Informationen nach Öffentlichkeitsprinzip möglicherweise private Interessen einer Drittperson betroffen, so muss das öffentliche Organ, welches für die Behandlung des Gesuches zuständig ist, der Drittperson Gelegenheit zur Stellungnahme geben. Denn sowohl Gesuchstellende als auch involvierte Drittpersonen können eine anfechtbare Verfügung verlangen, sollte das öffentliche Organ in Erwägung ziehen, gegen ihre Interessen zu entscheiden.

In einem Fall wurde anlässlich der Stellungnahme das E-Mail einer gesuchstellenden Person von der betroffenen Dienststelle tel quel an die involvierte Drittperson weitergeleitet. Damit verfügte die Drittperson über den Namen und die Kontaktdaten der gesuchstellenden Person. In der Folge hat die Drittperson mit der gesuchstellenden Person Kontakt aufgenommen. Die gesuchstellende Person wollte danach von der Aufsichtsstelle wissen, ob die Weiterleitung ihres E-Mails mit dem IDG vereinbar sei.

Das Recht auf Zugang zu Informationen gemäss § 23 IDG kann von jeder Person ohne Angaben von Gründen geltend gemacht werden. Weder die Person, die das Gesuch stellt, noch ihre Gründe sind für den Entscheid bedeutsam. Der Zugang zu Informationen kann eingeschränkt werden, wenn überwiegende öffentliche oder private Interessen vorliegen. Bei einer Interessenabwägung zählt allein das öffentliche Interesse an der Herausgabe der Information. Die Prüfung folgt dem Prinzip «access to one – access to all». Dies bedeutet, dass die Abwägung für «Jedermann» vorgenommen werden muss, unabhängig von der Person, die den Antrag gestellt hat. Deren privates Interesse am Erhalt der Information, ihre Motivation, ist für den Entscheid nicht massgebend.

In diesem Fall konnte die ASD bestätigen, dass eine Bekanntgabe der Identität der gesuchstellenden Person an die anzuhörende Person nicht notwendig war für die korrekte Durchführung des Verfahrens. Somit verletzte die Bekanntgabe die Bestimmungen des IDG. Die Kommunikation mit der Dienststelle ergab aber auch, dass sie nicht in böser Absicht gehandelt hatte, sondern der Ansicht war, dass damit das Verfahren beschleunigt werden könnte. Es ist durchaus denkbar, dass eine Privatperson einem Zugang zu Informationen weniger skeptisch gegenüber steht, wenn sie weiss, wer das Gesuch aus welchen Gründen gestellt hat. Der korrekte Weg hätte für die Dienststelle jedoch darin bestanden, vorgängig die gesuchstellende Person um ihre Einwilligung zu diesem Vorgehen zu bitten.

PUBLIKATION VERSCHIEDENER EINWOHNERDATEN IM GEMEINDEEIGENEN PUBLIKATIONSBLATT

Eine Gemeinde gelangte an die ASD und wollte wissen, ob sie sich richtig verhalte, wenn sie im gemeindeeigenen Publikationsblatt Zu- und Wegzug, Todesfall und Geburt nicht mehr veröffentliche. Bis Ende 2015 habe die Gemeinde diese Angaben publiziert, seither nicht mehr. Ein Einwohner der Gemeinde habe die Gemeindeverwaltung nun aufgefordert, diese Daten wieder im «Gmeiniblättli» zu veröffentlichen. Die Gemeinde stellte sich auf den Standpunkt, dass für die Publikation keine gesetzliche Grundlage bestehe.

Die ASD konnte der Gemeinde bestätigen, dass für solche Publikationen tatsächlich keine gesetzliche Grundlage besteht. Weil die Publikation der aufgeführten Daten auch nicht zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist, darf eine Publikation im «Gmeiniblättli» nur dann erfolgen, wenn vorgängig von der jeweils betroffenen Person eine Einwilligung eingeholt worden ist. Bei Neugeborenen müsste diese von den Erziehungsberechtigten abgegeben werden. Für die Publikation eines Todesfalles müsste die Einwilligung bei der verstorbenen Person bereits zu Lebzeiten eingeholt werden.

EINSICHT IN VORHANDENE PERSONENDATEN BEI EINER KANTONALEN SCHULE

Ein ehemaliger Schüler verlangte bei einer kantonalen Schule Einsicht in die vorhandenen Personendaten über ihn. Die Schule wollte das Gesuch abweisen.

Es stellte sich vorliegend die Frage des Zugangs zu den eigenen Personendaten nach § 24 IDG. Nach dieser Bestimmung hat jede Person Anspruch darauf zu wissen, ob bei einem öffentlichen Organ Daten über sie vorhanden sind, und gegebenenfalls auf Zugang zu diesen eigenen Personendaten. Der Zugang kann gemäss § 27 IDG eingeschränkt werden, wenn überwiegende private oder öffentliche Interessen dem entgegenstehen.

Als öffentliches Interesse kam hier die Wiederverwendung von Prüfungen in Frage. Bei diesen hätte der Zugang so eingeschränkt werden können, dass keine Kopien ausgehändigt würden, sondern die Einsichtnahme vor Ort erfolgen würde. Sofern auch Personendaten Dritter in den Aufzeichnungen vorhanden wären, wären auch ihre Interessen zu prüfen. Weitere Einschränkungsgründe waren keine erkennbar. Die ASD wies ausserdem darauf hin, dass der Zugang zu den eigenen Personendaten kostenfrei zu gewähren ist.

EINSICHT IN DIE JAHRESRECHNUNG EINER KESB DURCH EINE ANDERE KESB

Eine Kindes- und Erwachsenenschutzbehörde (KESB) des Kantons Basel-Landschaft gelangte mit der Frage an die ASD, ob sie einer anderen KESB des Kantons Einsicht in ihre Jahresrechnung gewähren müsse.

Im vorliegenden Fall stellte sich die Frage, ob die anfragende KESB gemäss § 23 Abs. 1 IDG Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen verlangen kann.

§ 23 Abs. 1 IDG statuiert, dass jede Person Anspruch auf Informationszugang hat. Bei der anfragenden KESB handelt es sich jedoch nicht um eine natürliche oder juristische Person im Sinne von § 23 Abs. 1 IDG, sondern um ein öffentliches Organ. Öffentliche Organe haben gemäss § 9 Abs. 1 IDG das Recht, von anderen öffentlichen Organen Personendaten zu erhalten, wenn ein Gesetz sie ausdrücklich dazu verpflichtet oder ermächtigt oder sie die Personendaten zur Erfüllung einer gesetzlichen Aufgabe brauchen. Eine solche gesetzliche Grundlage fehlte im vorliegenden Fall.

Die ASD stellte somit fest, dass der anfragenden KESB sowohl die Aktivlegitimation gemäss § 23 Abs. 1 IDG fehlte als auch eine gesetzliche Grundlage nach § 9 Abs. 1 IDG. Der Zugang konnte nicht gewährt werden.

LAUFENDE ZUSTELLUNG DER PROTOKOLLE DES SCHULRATES AN DIE PRÜFUNGS-KOMMISSIONEN EINER GEMEINDE

Das Präsidium eines Schulrates wollte von der ASD wissen, ob die Geschäftsprüfungs- und Rechnungsprüfungskommission der Gemeinde berechtigt seien, die jeweils neuesten Sitzungsprotokolle zu erhalten. Die Kommissionen machten geltend, dass sie die Protokolle für ihre Arbeit bräuchten.

Nach Prüfung der entsprechenden gesetzlichen Grundlagen im Gemeindegesetz gelangte die ASD zum Schluss, dass sich die Aufsichtstätigkeit der Prüfungskommissionen grundsätzlich auf abgeschlossene Fälle beziehe. In den Protokollen des Schulrates werden jedoch vornehmlich laufende Geschäfte diskutiert. Auch wenn die Prüfungstätigkeit der Kommissionen ihnen eine weitgehende Befugnis zum Informationsbezug einräumt, ist dabei stets auch das Verhältnismässigkeitsprinzip zu beachten. Die fortlaufende Zustellung der Schulratsprotokolle erwies sich somit als nicht ausreichend gesetzlich begründet sowie als unverhältnismässig.

Eine etwas andere Situation läge nach Einschätzung der ASD vor, wenn sich solche Protokolle zuverlässig anonymisieren liessen, da damit immerhin keine Personendaten weitergegeben würden. Gerade in einer kleineren Gemeinde ist aber eine Anonymisierung äusserst schwierig bis unmöglich.

AUFBEREITUNG VON FALLDATEN DER SOZIALHILFE EINER GEMEINDE DURCH DIE GEMEINDEVERWALTUNG

Eine Gemeindeverwaltung hat der kommunalen Sozialhilfestelle angeboten, deren Akten zuhanden des Gemeinderates elektronisch aufzubereiten. Bei Daten betreffend Massnahmen der sozialen Hilfe handelt es sich um heikle Daten, sogenannt «besondere Personendaten» im Sinne des Gesetzes. Dabei ist besonders darauf zu achten, dass nur jene Personen Kenntnis von solchen Personendaten erhalten, die sie wirklich zur Erfüllung ihrer gesetzlichen Aufgabe benötigen. Wenn immer möglich ist die Zahl der Personen, denen Personendaten bekanntgegeben werden, auf ein Minimum zu begrenzen. Da die kommunale Sozialhilfestelle die Aufbereitung der Daten selber vornehmen konnte, erwies sich der «Umweg» über die Gemeindeverwaltung als unnötig.

In diesem Zusammenhang möchte die ASD noch einmal darauf hinweisen, dass eine Gemeinde als Ganzes nicht ein «öffentliches Organ» im Sinne des IDG darstellt. Der Begriff «öffentliches Organ» orientiert sich an einzelnen, spezifischen Funktionen. Somit besteht eine Gemeinde aus verschiedenen «öffentlichen Organen» (Einwohnerdienste, Steuerbehörde, Sicherheit etc.). Werden Personendaten zwischen einzelnen kommunalen Abteilungen ausgetauscht oder bearbeitet, bedarf es deshalb in jedem einzelnen Fall einer gesetzlichen Grundlage.

BEKANNTGABE DES WEGZUGSORTS EINER EHEMALS IM EINWOHNERREGISTER VERZEICHNETEN PERSON TROTZ SPERRUNG

Eine Gemeinde gelangte an die ASD, weil sie von einem Finanzinstitut um Auskunft über den Wegzugsort einer ehemals in der Gemeinde wohnhaften Person gebeten worden war. Das Finanzinstitut wollte die Angaben, um mit der Person weiterhin einen Kundenkontakt pflegen zu können. Die betroffene Person hatte ihre Daten bei der Gemeinde allerdings sperren lassen.

Die ASD teilte der Gemeinde mit, dass die Gemeinde dem Finanzinstitut die Angaben nicht liefern dürfe, da die Voraussetzungen von § 26 Abs. 3 IDG nicht erfüllt seien. Damit eine Datensperre durchbrochen werden kann, muss die um Bekanntgabe ersuchende Person glaubhaft machen können, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind. Der Wunsch nach blossem Kundenkontakte erfüllt diese Voraussetzung nicht.

BEKANNTGABE VON PERSONENDATEN AN EINE PERSON AUS DEM AUSLAND

Eine Gemeinde wurde von einem Rechtsanwalt um die Adresse eines Einwohners angefragt, um gegen diesen rechtlich vorzugehen zu können. Sowohl der Rechtsanwalt als auch sein Mandant hatten ihren (Wohn-)Sitz in Deutschland. Die Gemeinde wollte von der Aufsichtsstelle wissen, ob dieser Umstand bei der Prüfung des Gesuchs eine Rolle spiele oder einer Bekanntgabe gar entgegenstehen könnte.

Auch bei Anfragen aus dem Ausland muss zuerst die rechtliche Grundlage für die Weitergabe von Daten geprüft werden. Sodann muss abgeklärt werden, welche Bedingungen für das konkrete Land, aus dem das Gesuch stammt, gelten. Das IDG schreibt für einen solchen Fall vor, dass abhängig vom Empfängerland unterschiedliche Massnahmen zur Wahrung eines angemessenen Schutzes zu treffen sind. Die Prüfung verläuft also zweiteilig. Erstens wird die grundsätzliche Rechtmässigkeit der Bekanntgabe geprüft, danach die Art der Übermittlung.

Im vorliegenden Fall schränkt die gesetzliche Grundlage gemäss Anmelde- und Registergesetz (ARG) den Kreis der Empfänger nicht auf Personen in der Schweiz ein. Die Gemeinde hat korrekt festgestellt, dass die rechtlichen Voraussetzungen für die Herausgabe der Daten erfüllt waren. Demnach musste nur noch geprüft werden, welche Regelung für Deutschland gilt. Für den Datenaustausch mit Deutschland als Staat, welcher der Europaratskonvention K-108 beigetreten ist, sind nach § 21 Abs. 1 IDG bezüglich Bekanntgabe von Daten keine zusätzlichen Schutzmassnahmen nötig. Die Herausgabe von Daten ist also rechtens.

Die ASD betont an dieser Stelle, dass damit nur gesagt ist, dass die Personendaten auf dem gleichen Weg bekannt gegeben werden können, wie wenn sich der Empfänger oder die Empfängerin in der Schweiz aufhalten würde. Auch bei einem Datentransfer ins Ausland muss aber je nach Schutzbedarf der Information die Bekanntgabe auf sicherem Weg erfolgen.

VIDEOÜBERWACHUNG DER ENTSORGUNGS- UND ABFALLSTELLEN IN EINER GEMEINDE

Eine Gemeinde gelangte an die ASD, da sie die Absicht hatte, ihre Entsorgungs- und Abfallstellen per Video zu überwachen. Dies deshalb, weil an den Stellen regelmässig illegal Abfall entsorgt wurde und die Gemeinde bisher erfolglos versucht hatte, dem Problem mit anderen Massnahmen zu begegnen.

Seit dem 1. Januar 2015 besteht im Kanton Basel-Landschaft im Polizeigesetz (PolG) eine gesetzliche Grundlage für die personenbezogene Videoüberwachung des öffentlichen Raums. Nach § 45d Abs. 1 und 2 PolG können die Direktionen, die Landeskanzlei, das Kantonsgericht, die selbständigen Verwaltungsbetriebe sowie die Gemeinden – zum Schutz von Angestellten oder von Objekten und in ihrem jeweiligen Verantwortlichkeitsbereich – eine örtlich begrenzte Überwachung allgemein und nicht allgemein zugänglicher öffentlicher Orte mit Videokameras vorsehen, welche die Personenidentifikation zulassen. Dabei darf die Videoüberwachung nur die Verhinderung und Ahndung von Straftaten bezwecken. Sie muss zudem verhältnismässig sein, d.h. geeignet sein, Straftaten zu verhindern oder deren Ahndung zu erleichtern, und deren Zweck darf nicht durch eine mildere Massnahme erreicht werden. Darüber hinaus sieht § 45d Abs. 3 PolG zwingend vor, dass das öffentliche Organ, welches eine Videoüberwachung betreiben möchte, für jede Überwachungsanlage ein sogenanntes Betriebsreglement bzw. eine Betriebsordnung erlässt. Darin müssen der Zweck der Überwachungsanlage, die Beschreibung des überwachten Perimeters, die Dauer und Einschaltzeiten der Überwachung, die Standorte der Videokameras, die Massnahmen am bewachten Ort zum Hinweis auf die Überwachung, die Beauftragung einer klar bestimmten und geringen Anzahl von Mitarbeitenden mit der Auswertung, die Speicherung und Vernichtung der Videoaufzeichnungen, die regelmässige Überprüfung der Datenschutzbestimmungen sowie die Regelung des physischen und elektronischen Zugangs zu den Videoaufzeichnungsdaten, Kopien

und Ausdrucken abschliessend geregelt werden. Anders als in anderen Kantonen sind die Installation und der Betrieb einer personenbezogenen Videoüberwachung im Kanton Basel-Landschaft nicht von einer Bewilligung durch die ASD abhängig.

Die ASD konnte anlässlich einer Besprechung mit Vertretern der Gemeinde Unklarheiten bezüglich der konkreten Ausgestaltung der Betriebsordnung sowie der Installation der Videoüberwachung klären. So sollen die Sammelstellen alternierend und lediglich zu bestimmten Zeiten mit einer mobilen Kamera videoüberwacht werden. Die bestehenden Hinweisschilder mit den Betriebszeiten der Sammelstellen sollen mit Hinweisen zur Videoüberwachung ergänzt werden.

Die ASD möchte darauf hinweisen, dass eine Videoüberwachung einen starken Eingriff in die Privatsphäre der überwachten Bürgerinnen und Bürger darstellt. Wenn öffentlicher Grund überwacht wird, so ist die Zahl der möglichen Betroffenen besonders hoch. Zudem bleibt den Überwachten oft keine Wahl, ob sie den überwachten Bereich betreten wollen oder nicht. Eine Videoüberwachung auf öffentlichem Grund muss deshalb immer gut überlegt sein und sollte nicht leichtfertig eingesetzt werden.

AUF WOLKE SIEBEN?

Im Berichtsjahr hat die ASD ein erhöhtes Bedürfnis nach Beratung für die Nutzung von Cloud-Diensten festgestellt. Vor allem für kleinere Behörden wie zum Beispiel Gemeinden oder Kreisschulen, die im Gegensatz zur kantonalen Verwaltung über keinen zentralen internen IT-Dienstleister verfügen, sind Cloud-Lösungen verlockende, vermeintlich unkomplizierte und in kurzer Zeit umsetzbare Betriebsvarianten.

Die ASD wurde um Stellungnahmen zu verschiedenen Cloud-Angeboten gebeten. Sie wies stets darauf hin, dass für die Abschätzung der mit der Cloud-Nutzung verbundenen Risiken als Erstes der Schutzbedarf der betroffenen Personendaten ermittelt werden muss. Sollen besondere Personendaten[1] in der Cloud bearbeitet werden, so besteht die technische Herausforderung darin, dass das Schlüsselmanagement der Datenverschlüsselung beim verantwortlichen Organ bleiben muss. In jedem Fall ist bei einer Personendatenbearbeitung in der Cloud eine vertragliche Vereinbarung mit dem Cloud-Anbieter nötig. Diese Vereinbarung muss u.a. Gerichtsstand, Ort der physischen Speicherung, Schlüsselhandling, Subunternehmen und Weisungs- und Kontrollbefugnisse regeln.

Da immer mehr Schulen den Einsatz von Office 365 aus der Microsoft-Cloud für den Einsatz im Unterrichtsumfeld prüfen, hat privatim (Konferenz der schweizerischen Datenschutzbeauftragten) und educa.ch zusammen mit Microsoft Vertragsbedingungen erarbeitet, damit Schulen die gängigsten Onlinedienste datenschutzkonform nutzen können. Diese Vertragsbedingungen erlangen nur bei einem Beitritt zum Rahmenvertrag zwischen educa.ch und Microsoft Gültigkeit. Die Schulen müssen bei der Einrichtung der Onlinedienste darauf achten, dass sie ein Rechenzentrum mit Standort in der Schweiz oder der Europäischen Union auswählen und dass der Gerichtsstand in der Schweiz liegt. Auch bei den Schulen gilt jedoch, dass besondere Personendaten wie zum Beispiel Krankmeldungen, Meldungen an die KESB sowie andere streng vertrauliche Informationen nicht in der Cloud abgelegt werden dürfen – ausser, sie werden *vor* einer Ablage zusätzlich angemessen verschlüsselt.

1] Besondere Personendaten sind gemäss § 3 Abs. 4 IDG:

a. Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über:
   1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oderTätigkeiten,
   2. die Gesundheit, das Erbgut, die Intimsphäre oder die Rassenzugehörigkeit,
   3. Massnahmen der sozialen Hilfe,
   4. administrative oder strafrechtliche Verfolgungen und Sanktionen.

b. Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Persönlichkeitsprofil).

Da im Gegensatz zum Unterrichtsumfeld im Schulverwaltungsumfeld davon auszugehen ist, dass Personendaten der Kategorie «besondere Personendaten» bearbeitet, gesendet und empfangen werden, riet die ASD im Berichtsjahr von einer breiten Nutzung von Cloud-Lösungen wie z.B. Office 365 im Schulverwaltungsalltag ab. Der verschlüsselte Empfang von besonderen Personendaten ausserhalb des Einflussbereichs der Schule kann nicht beeinflusst werden. Die manuelle Verschlüsselung gestaltet sich dort eher benutzerunfreundlich und wird deshalb möglicherweise umgangen. Die ASD kam zum Schluss, dass Office 365, iCloud und weitere Cloud-Anbieter für einen einfachen Einsatz in der Verwaltung mit potentiell vertraulichen Daten im Mail und in der Dateiablage aktuell noch nicht einsatzbereit sind. Sie hofft für die Zukunft auf datenschutzkonforme Angebote und die Entwicklung praktikabler Verschlüsselungslösungen, welche es öffentlichen Organen ermöglichen, ihre Verantwortung bei der Einhaltung der datenschutzrechtlichen Bestimmungen wahrzunehmen.

VORABKONTROLLE

VORABKONTROLLE: VORBEUGEN IST EINFACHER ALS HEILEN

Die datenschutzrechtliche Vorabkontrolle ist ein präventives Instrument, mit der die Aufsichtsstelle überprüft, ob geplante Datenverarbeitungen von öffentlichen Organen mit den Anforderungen an den Datenschutz und die Informationssicherheit vereinbar sind. Sie ist immer dann nötig und gesetzlich vorgeschrieben, wenn geplante Datenverarbeitungen besondere Risiken für die Rechte und Freiheiten von Betroffenen mit sich bringen können. Die Erfahrung zeigt, dass nachträgliche Nachbesserungen in der Regel kostenintensiver sind oder sich im schlechtesten Fall nicht mehr umsetzen lassen. Ein frühzeitiger Einbezug der Aufsichtsstelle in ein Projekt hilft, unnötige Verzögerungen in der Einführungsphase oder im Betrieb zu verhindern. Die Aufsichtsstelle hat im Berichtsjahr für solche Vorabklärungen einen grossen Teil der dafür zur Verfügung stehenden Ressourcen aufgewendet.

Auf der Basis von gesetzlich festgelegten Risikokriterien entscheidet die Aufsichtsstelle, ob eine Vorabkontrolle durchzuführen ist. Nicht nur bei neuen Datenbearbeitungen, d.h. Einführung neuer Systeme, sondern auch bei gravierenden Änderungen von bestehenden Datenbearbeitungen mit besonderen Risiken sollte bei der Aufsichtsstelle abgeklärt werden, ob eine Vorabkontrolle durchgeführt werden muss oder nicht. Mit neuen IT-Systemen entstehen möglicherweise neue Risiken und Verwundbarkeiten, Versäumnisse bestehender Lösungen könnten behoben, neue Massnahmen und Kontrollmechanismen verankert werden. So kann auch eine vermeintlich lapidare Ergänzung einer Datenbank um ein Datenfeld mit Personenbezug eine Neubeurteilung des Schutzbedarfs nötig machen. Für Vorabkontrollen müssen dabei nicht immer alle Projektdokumente vorgelegt werden. Die Aufsichtsstelle klärt jeweils mit den Projektverantwortlichen, welche Dokumente in welcher Phase zur Prüfung vorgelegt werden müssen. Welche Dokumente dies betrifft, hängt auch davon ab, ob die Vorabkontrolle in einem Prüfungsschritt oder in mehreren Schritten durchgeführt wird und welche spezifischen Risiken ein Projekt birgt. Nicht zuletzt ist der Ablauf der Verfahren auch von den Ressourcen abhängig, welche der Aufsichtsstelle zur Verfügung stehen.

Bisher betrafen sämtliche Vorabkontrollen öffentliche Organe der kantonalen Verwaltung. Neu wurden im Berichtsjahr auch drei Gesuche um Vorabkontrollen aus dem Schulbereich und dem Gesundheitswesen eingereicht. Im Berichtsjahr gingen insgesamt acht Projekte zur Vorabkontrolle ein. Sechsundzwanzig Projekte aus dem Vorjahr wurden im Berichtsjahr weiterbearbeitet oder waren in Prüfung – mehr als doppelt so viele wie im Vorjahr. Die hohe Zahl von parallel laufenden Vorabkontrollen gefährdet die beabsichtigten Fristen bis zur Stellungnahme der Aufsichtsstelle.

Bei insgesamt sieben Projekten 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. In einem dieser Fälle wurden die Projektverantwortlichen stattdessen bei der Vertragsgestaltung mit dem Outsourcing-Partner beraten. 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.

Der Prozess der Vorabkontrolle endet mit der abschliessenden Stellungnahme der Aufsichtsstelle. Die Vorabkontrolle sollte vor der Realisierung des Projekts erfolgen, damit die Empfehlungen noch umgesetzt werden können. Findet eine Inbetriebnahme der geplanten Datenbearbeitung vor Abschluss der Vorabkontrolle statt, ohne dass die Verantwortlichen den Abschluss der Vorabkontrolle abgewartet haben, führt die Nichteinhaltung von § 12 IDG zu einem Abbruch der Vorabkontrolle. Im Berichtsjahr betraf dies drei Projekte, in welchen mangelndes Risikobewusstsein verbunden mit Projektzeitdruck zur Umsetzung von Lösungen führte, ohne dass die erhöhten Risiken genauer analysiert wurden oder die Verantwortlichen ihnen mit angemessenen Massnahmen begegnet wären. Konkret wurden so eine Vorabkontrolle in der Sicherheitsdirektion (SID) und zwei Vorabkontrollen zu Cloud-Projekten in der Bildungs-, Kultur- und Sportdirektion (BKSD) vorzeitig abgebrochen. Bei den Cloud-Projekten verstärkte sich der Zeitdruck durch den Wunsch der Anwenderinnen und Anwender, auch im beruflichen Alltag die Tools einsetzen zu können, die sie trotz Cloud-Risiken privat bereits nutzten. Dabei ging vergessen, dass anders als im privaten Umfeld in der öffentlichen Verwaltung fremde Personendaten bearbeitet werden und die gesetzlichen Vorgaben einzuhalten sind.

Die Aufsichtsstelle verfasste im Berichtsjahr elf Stellungnahmen, teilweise mehrere zu einem Projekt in verschiedenen Phasen. Schwerpunktmässig zeigte sich auch in diesem Berichtsjahr bei den vorab geprüften Vorhaben Handlungsbedarf bei der Methodik der Rechtsgrundlagenanalyse, der risikobasierten Konzeption der Sicherheitsmassnahmen im mobilen Umfeld, im Zusammenhang mit Cloud-Lösungen sowie bei Berechtigungskonzepten und Outsourcing-Verträgen.

Die ASD hatte es im Berichtsjahr regelmässig mit Projekten zu tun, bei denen die Beteiligten mit der Rechtsgrundlagenanalyse oder der Risikoanalyse und der Konzeption von Sicherheitsmassnahmen nicht ausreichend vertraut waren, da sie darin bisher weder geschult worden waren noch Erfahrung gesammelt hatten. Dies führte unter anderem dazu, dass die Aufsichtsstelle Datenschutz vor den eigentlichen Vorabkontrollen die Stellen erst einmal beraten hat. Besonders intensiv war dies im Berichtsjahr bei zwei Cloud-Projekten, einem Geschäftsverwaltungsprojekt und einem Mobile-Computing-Projekt der Fall. Die ASD hat ausserdem die Fachstelle Kantonales Personenregister (arbo) beratend unterstützt, für den Standardfall eines externen Anschlusses an das Personenregister ein Raster zu erstellen. Die so entstandenen Dokumentvorlagen entlasten sowohl die Behörden bei der Konzeption der Sicherheitsmassnahmen als auch die Aufsichtsstelle bei der späteren Vorabkontrolle. Oftmals gewünschte Leistungen in Form der Erarbeitung von Dokumenten wie die einer Rechtsgrundlagenanalyse bzw. eines ISDS-Konzeptes kann die ASD jedoch aufgrund ihrer Rolle nicht erbringen, da sie die entsprechenden Grundlagen danach als Aufsichtsorgan selbst kontrollieren muss.

Für die Projektmitarbeitenden ist es nach wie vor schwierig, aus dem Schutzbedarf der Informationen eine authentische Risikoanalyse zu erstellen und daraus angemessene Schutzmassnahmen zu konzipieren. Die Aufsichtsstelle arbeitet deshalb eng mit dem Kantonalen Sicherheitsbeauftragten zusammen, um einen Beitrag zur Verbesserung der methodischen Hilfestellungen zu leisten.

Im Berichtsjahr hat die ASD einen «Leitfaden Berechtigungskonzept» veröffentlicht, der den verantwortlichen Stellen einerseits eine Hilfestellung geben soll, wie sie ihre Berechtigungskonzepte gestalten und umsetzen können. Andererseits dient er den Projektmethodik-Verantwortlichen, Projektmitarbeitenden entsprechende Vorlagen und Hilfsmittel zur Verfügung zu stellen. In der kantonalen Verwaltung des Kantons Basel-Landschaft wurde damit im Berichtsjahr begonnen.

Positiv ist zu vermerken, dass die Erkenntnis spürbar zunimmt, dass es sich lohnt, die Aspekte von Datenschutz und Informationssicherheit frühzeitig zu berücksichtigen. Dadurch wird die Qualität der Projekte bzgl. Datenschutz und Informationssicherheit erhöht. Gleichzeitig wird der Aufwand der Projektleitenden und der Aufsichtsstelle minimiert, woraus sich eine Win-Win-Situation ergibt, die letztlich den von der Datenbearbeitung betroffenen Personen, aber auch dem öffentlichen Organ zugutekommt.

KONTROLL-TÄTIGKEIT

Die Aufsichtsstelle Datenschutz pflegt eine rollende, risikobasierte Kontrollplanung. Die rollende Planung führt dazu, dass die Planungen der Kontrolle und deren Durchführung nicht zwingend im selben Jahr stattfinden. Ebenfalls zur Kontrolltätigkeit zählt die Prüfung des Reportings zur Umsetzung der Empfehlungen aus kürzlich erfolgten Kontrollen. Die Effizienz dieses Prozesses hängt vom Verantwortungsbewusstsein der kontrollierten Behörden ab. Da im Berichtsjahr noch mehr Projekte als im Vorjahr zur Vorabkontrolle eingereicht wurden, verblieben der Aufsichtsstelle wenig Ressourcen für eigentliche Kontrollen, weshalb im Berichtsjahr nur eine Kontrolle durchgeführt werden konnte.

Die Berichte, welche die ASD im Rahmen ihrer Kontrolltätigkeit erstellt oder erstellen lässt, sind samt den ihnen zugrunde liegenden Materialien nicht öffentlich (§ 41 Abs. 3 IDG). Dies einerseits, um einen möglichst vertrauensvollen Informationsfluss mit dem kontrollierten öffentlichen Organ zu ermöglichen und somit die Grundlage zu schaffen, damit Schwachstellen identifiziert und behoben werden können. Andererseits soll vermieden werden, dass mit einer Publikation von Schwachstellen das Risiko eines Angriffs eingegangen wird.

AMT FÜR LEBENSMITTEL-SICHERHEIT UND VETERINÄRWESEN (ALV)

Aus datenschutzrechtlicher Sicht vereinen die Tätigkeiten des Amtes für Lebensmittelsicherheit und Veterinärwesen (ALV) verschiedene Risiken für die Rechte und Freiheiten von Betroffenen: so zum einen die Datenbearbeitung besonderer Personendaten, insbesondere in der Form von Informationen über administrative und strafrechtliche Verfolgungen und Sanktionen. Neben einem weiteren Risiko durch sogenannte Abrufverfahren bergen auch organisatorische Änderungen durch die Zusammenlegung zweier Ämter mit unterschiedlichen Aufgaben (Lebensmittelsicherheit und Veterinärwesen) entsprechende Risiken. Hat eine Organisationseinheit mehrere gesetzliche Aufgaben zu erfüllen und werden diese Aufgaben durch verschiedene Abteilungen erfüllt, so werden diese datenschutzrechtlich als funktionale Behörden mit entsprechender Verantwortung im Sinne von § 6 IDG betrachtet. Sie sind zwar hierarchisch der gleichen (Amts-)Leitung unterstellt, jedoch muss sich der unterschiedliche Aufgabenbereich gestützt auf unterschiedliche gesetzliche Grundlagen in der Trennung der zu bearbeitenden Personendaten abbilden, letztlich auch in entsprechenden Berechtigungskonzepten.

Aus diesen Gründen wurde das ALV schon 2016 für eine datenschutzrechtliche Kontrolle ausgewählt. Die Kontrolle vor Ort wurde im Berichtsjahr durchgeführt und mit einem Schlussbericht im gleichen Jahr abgeschlossen.

Schwerpunkte der datenschutzrechtlichen Kontrolle waren, den potentiellen Risiken entsprechend, der Informationsfluss bzw. die Zugriffsrechte innerhalb des ALV, der Umgang mit besonderen Personendaten sowie organisatorische

und technische Massnahmen zur Wahrung des Datenschutzes und der Informationssicherheit. Ausserdem prüfte die Aufsichtsstelle standardmässig die Umsetzung weiterer datenschutzrechtlicher Vorgaben wie z.B. Verhältnismässigkeit, Aufbewahrung und Löschung von Daten.

Im Rahmen der Kontrolle fiel positiv auf, dass das ALV in seinen Kernaufgaben sehr transparente Prozessdokumentationen und definierte Abläufe erstellt, was auch der Transparenz der Datenbearbeitung zuträglich ist. Ausserdem waren anlässlich der Kontrolle keine Anzeichen zu erkennen, dass Personendaten zu anderen als den gesetzlich vorgesehenen Zwecken verwendet worden sind. Trotzdem hat die ASD bei ihrer datenschutzrechtlichen Kontrolle festgestellt, dass gewisse gesetzliche Anforderungen des Datenschutzes und der Informationssicherheit bei der Datenbearbeitung teilweise nicht angemessen erfüllt wurden und entsprechend Handlungsbedarf bestand, um ein angemessenes Niveau hinsichtlich Datenschutz und Informationssicherheit zu erreichen. Die Kontrolle ergab sieben Feststellungen zu dringlich zu behebenden Schwachstellen und zehn Schwachstellen, welche ein mittleres Risiko bargen. Eine Feststellung wurde als Optimierungspotential ausgewiesen.

Dringenden Handlungsbedarf sah die ASD namentlich betr. Verhältnismässigkeit im Sinne von § 9 Abs. 3 des IDG. Dort identifizierte die ASD Bereiche, welche mit unverhältnismässigen Zugriffsrechten nicht dem Need-to-know-Prinzip folgten. Gleiches gilt bezüglich der ungenügenden Umsetzung der Vorgaben im Bereich Informationssicherheit und damit der Einhaltung von § 8 IDG. Dass diesbezüglich das Bewusstsein für Informationssicherheit nicht genügend vorhanden war, hängt sicher auch damit zusammen, dass der Volkswirtschafts- und Gesundheitsdirektion (VGD) zu wenig Ressourcen des für sie zuständigen Sicherheitsbeauftragten zur Verfügung stehen. So hatte das ALV bis zur datenschutzrechtlichen Kontrolle noch keinen Kontakt mit dem Sicherheitsbeauftragten.

Das ALV hat bereits im Anschluss an die Kontrolle mit der Behebung der Schwachstellen begonnen, die genannten Feststellungen beziehen sich gemäss Revisionsstandard auf den Zeitpunkt der Kontrolle.

ÖFFENTLICHKEITS-PRINZIP

Die Landeskanzlei hat in Nachachtung von § 13 Abs. 6 der Verordnung zum IDG (IDV) der Aufsichtsstelle Datenschutz die folgenden Zahlen der bei den Direktionen im Berichtsjahr eingegangenen Gesuche um Zugang zu Informationen gemeldet.

Direktion	Anzahl Gesuche	Vorjahr	Gutgeheissen	Teilweise gutgeheissen	Abgewiesen
BKSD	4	24	1	3	0
BUD	3	4	2	0	1
FKD	1	3	0	0	1
SID	3	4	2	1	0
VGD	5	3	4		1
LKA	1	0	0	0	1
Total	**17**	**38**	**9**	**4**	**4**

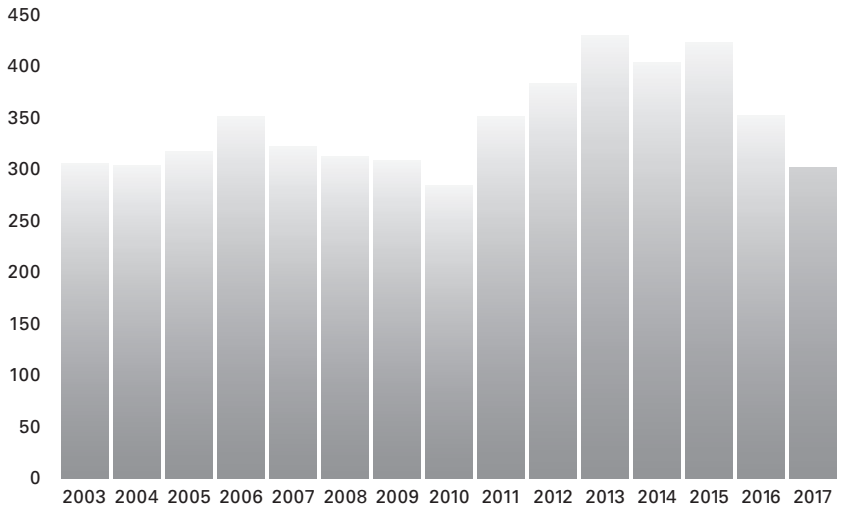
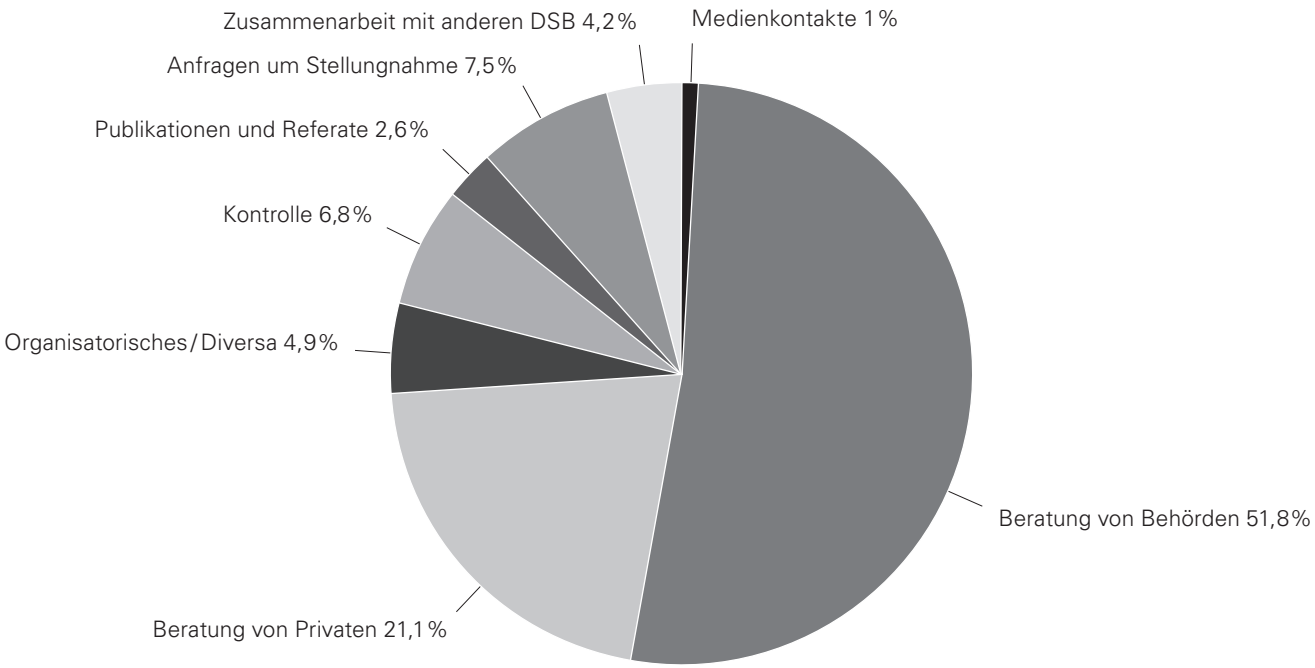
Die Zahlen zeigen einen deutlichen Rückgang der Gesuche gegenüber dem Vorjahr. Dieser Rückgang ist darauf zurückzuführen, dass im Berichtsjahr erstmals jene Gesuche nicht erfasst wurden, die kein Gesuch im Sinne des Öffentlichkeitsprinzips gemäss § 23 IDG waren. Gesuche um Zugang zu Informationen können sich auf verschiedene rechtliche Grundlagen stützen. Neben der verfahrensrechtlichen Akteneinsicht gehen bei der Verwaltung auch immer wieder Gesuche um Zugang zu den eigenen Personendaten gemäss § 24 IDG ein. Auch wenn der Zugang zu «allgemeinen» Informationen und jener zu den eigenen Personendaten beide im IDG geregelt sind, ist der Zweck der Bestimmungen ein völlig anderer. Die Möglichkeit des Zugangs zu den eigenen Personendaten ist ein in den Datenschutzgesetzen schon lange bestehendes Recht für Einzelpersonen, sich zu informieren, welche Daten über sie bearbeitet werden.

Das Recht auf Zugang zu bei den öffentlichen Organen vorhandenen Informationen (§ 23 IDG) hingegen wird vereinfacht als «Öffentlichkeitsprinzip» bezeichnet. Das Ziel ist die Transparenz der Verwaltungstätigkeit, was eine Voraussetzung für die Wahrung der demokratischen Rechte ist.

Die diesjährigen Zahlen müssen mit Vorsicht interpretiert werden. Insbesondere der starke Rückgang der Gesuche in der BKSD ist auf die Änderung der Erhebung zurückzuführen. Unter Berücksichtigung der Anpassung bei der Erhebung ist gegenüber dem Vorjahr wiederum eine leichte Zunahme der Gesuche festzustellen. Mit diesem geringen Anstieg liegt der Kanton Basel-Landschaft im schweizerischen Trend. Aus Sicht der Transparenz ist sicher hervorzuheben, dass lediglich vier Gesuche vollständig abgewiesen werden mussten, wobei in zwei Fällen formale Gründe vorlagen. In einem Fall war der Bund zuständig, im zweiten lag die Information gar nicht vor.

ANHANG

GESCHÄFTE



ART DER GESCHÄFTE