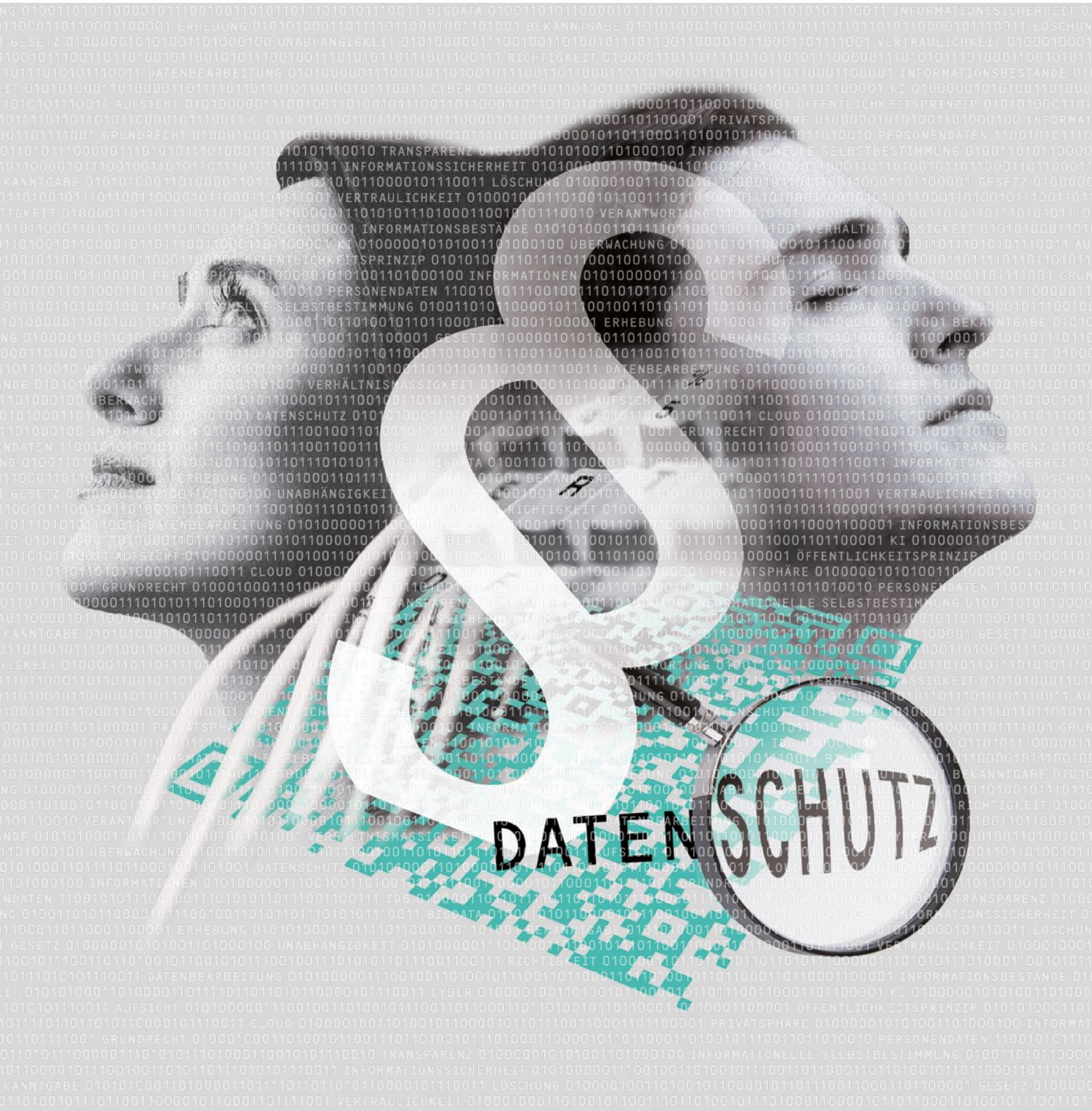
BASEL LANDSCHAFT

TÄTIGKEITSBERICHT 2019
DER AUFSICHTSSTELLE DATENSCHUTZ



AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragter:
Markus Brönnimann

Stv. Datenschutzbeauftragter:
Tobias Schnelli

Akademische Mitarbeitende:
Priscilla Dipner-Gerber
Ditmar Freitag
Thomas Held

Büro:
Rathausstrasse 45
4410 Liestal
Telefon: +41 (0)61 552 64 30
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.

INHALTSVERZEICHNIS

1

DAS JAHR 2019

1.1 DIE AUFSICHTSSTELLE DATENSCHUTZ (ASD)

Die ASD ist eine unabhängige Aufsichtsbehörde. Sie verfügt über fundiertes Fachwissen bezüglich Datenschutz, dem Umgang mit Informationen und Informationssicherheit. Als unabhängige Aufsichtsbehörde ist die ASD, wie beispielsweise auch der Ombudsman oder die Finanzkontrolle, nicht dem Regierungsrat des Kantons unterstellt und erfüllt ihre Aufgaben weisungsunabhängig.

Dem gesetzlichen Auftrag entsprechend hat die ASD im Berichtsjahr bei den öffentlichen Organen unseres Kantons Beratungen, Vorabkontrollen, Kontrollen und Schulungen durchgeführt und zu datenschutzrelevanten Erlassen Stellung genommen. Zu den öffentlichen Organen zählen die Kantonsverwaltung, die Gemeinden, öffentliche Institutionen sowie Private, die eine öffentliche Aufgabe übernehmen. Ebenfalls berät und unterstützt die ASD Betroffene bei der Wahrnehmung ihrer Rechte bezüglich Datenschutz und Öffentlichkeitsprinzip. Selbstverständlich umfasste ihr Angebot auch Auskünfte an und fachlich fundierte Einschätzungen für Landrat und Medien.

Im Berichtsjahr hat die ASD 451 Dossiers eröffnet. Dies stellt in der Geschichte der ASD einen neuen Rekord dar und bedeutet eine Zunahme von knapp 10% im Vergleich zum Vorjahr. Der Aufsichtsstelle wurden 32 neue Vorhaben zur Vorabkontrolle vorgelegt. Bei zehn Vorhaben entschied die ASD, keine Vorabkontrolle durchzuführen. Bei drei weiteren Vorhaben wurde keine Vorabkontrolle durchgeführt, da diese zu spät im Projektablauf vorgelegt wurden und die Empfehlungen im Projekt keine Wirkung mehr hätten entfalten können. Es wurden drei Datenschutzkontrollen abgeschlossen, 183 Beratungen bei öffentlichen Organen und 112 bei Privaten durchgeführt sowie elf Schulungen und Referate gehalten. Die ASD wurde für 55 Stellungnahmen angefragt und verfasste weitere 25 Stellungnahmen im Rahmen von Vorabkontrollen.

Der ASD standen für diese Aufgaben 360 Stellenprozente zur Verfügung, welche auf fünf Personen verteilt waren. Ausserdem bot sie eine Volontariatsstelle für Juristen und Juristinnen an.

1.2 RESSOURCEN

Der Landrat hat mit dem im Berichtsjahr verabschiedeten Budget die personellen Ressourcen für den Datenschutz um eine Stelle aufgestockt. Er unterstreicht damit, dass die Bedeutung des Datenschutzes und der Informationssicherheit – u. a. aufgrund der fortschreitenden Digitalisierung – steigt und dass die diesbezüglichen Herausforderungen in unserem Kanton ernst genommen werden. Wir danken an dieser Stelle für das Vertrauen und die Wertschätzung unserer Arbeit.

1.3 DER DATENSCHUTZ

Die Begriffe «Datenschutz» und «Datensicherheit» werden umgangssprachlich oft synonym verwendet. Datensicherheit ist ein Teilaspekt der Informationssicherheit. Beim Datenschutz handelt es sich um den Schutz aller Personen vor Missbrauch ihrer persönlichen Daten – den Schutz der Privatsphäre – gemäss Art. 13 Abs. 2 der seit 1999 geltenden Bundesverfassung (BV). Bereits vor der neuen Verfassung war dieses Recht anerkannt, wurde aber von der Rechtsprechung als Teil der persönlichen Freiheit ausgelegt. Seit der Revision der Bundesverfassung ist der Schutz der persönlichen Daten nun auch «offiziell» ein Grundrecht, wie es etwa auch die persönliche Freiheit selbst, das Recht auf Leben, das Folterverbot oder auch die Meinungs- und Informationsfreiheit sind. Sämtliche staatlichen Akteure sind verpflichtet, dafür zu sorgen, dass die Grundrechte in der gesamten Rechtsordnung zur Geltung kommen.

Grundrechte sind staatlich garantierte Freiheits- und Gleichheitsansprüche, die allen Menschen zustehen. Sie sind vor Gericht einklagbar. Zusätzlich werden die Grundrechte auch über den Beitritt der Schweiz zur Europäischen Menschenrechtskonvention (EMRK) geschützt.

Die meisten Grundrechte gelten nicht absolut und können unter bestimmten Umständen eingeschränkt werden. Dies gilt auch für den Schutz der Privatsphäre. Denn Grundrechte können einerseits miteinander kollidieren oder andererseits die legitime Aufgabenerfüllung des Staates verhindern. Sie müssen somit in gewissen Fällen eingeschränkt werden können. Die Grundsätze einer Beschränkung eines Grundrechts sind in Art. 36 BV festgehalten. Einschränkungen müssen sich auf eine hinreichende gesetzliche Grundlage stützen. Sie müssen durch ein überwiegendes öffentliches

Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt sein und sie müssen verhältnismässig (geeignet, notwendig und für die betroffenen Personen zumutbar) sein. Die Grundsätze der Grundrechte regeln demnach nicht das komplexe Zusammenspiel, sondern es bedarf zusätzlich einer Fülle von ergänzenden gesetzlichen Bestimmungen. Dies gilt auch für den Schutz vor Missbrauch der persönlichen Daten, oder die sogenannte «informationelle Selbstbestimmung». Es liegt auf der Hand, dass der Staat zahlreiche Daten der Einwohnerinnen und Einwohner benötigt, um seine Aufgaben zu erfüllen.

Zur Regelung der staatlichen Datenbearbeitung legt der Gesetzgeber in den Datenschutzgesetzen die Voraussetzungen und Grundsätze der Datenbearbeitung fest. Das Informations- und Datenschutzgesetz Basel-Landschaft (IDG) regelt in allgemeiner Weise die Pflichten der Behörden, die Rechte der betroffenen Personen, die Anforderungen an die Informationssicherheit sowie die Aufsicht.

Das formelle Datenschutzrecht gibt aber keine Auskunft darüber, welche Daten konkret von einem öffentlichen Organ bearbeitet werden dürfen. Dies ist die Aufgabe des Sachrechts. Die Sachgesetzgebung beschäftigt sich mit der konkreten Aufgabenerfüllung und muss jeweils für ihren Fachbereich definieren, welche Daten für die Aufgabenerfüllung notwendig sind, woher sie bezogen werden und wem sie allenfalls weiter bekanntgegeben werden dürfen. Idealerweise lässt sich die Datenbearbeitung unmittelbar den gesetzlichen Grundlagen entnehmen, indem sie möglichst präzise festgelegt wird. Oftmals ist die gesetzliche Grundlage jedoch nur eine mittelbare, indem das Gesetz oder die Verordnung lediglich die öffentliche Aufgabe nennt und daraus das Recht zur Bearbeitung der Daten anhand der Notwendigkeit abgeleitet werden muss.

Für jede Bearbeitung von Personendaten gilt jedoch, dass sie in Fällen, in welchen sie sich nicht auf eine gesetzliche Grundlage stützen kann, unrechtmässig ist und somit einen unerlaubten Eingriff in ein Grundrecht darstellt.

Das Recht auf Privatsphäre ist wichtig, da es u. a. sicherstellen soll, dass wir nicht einfach überwacht werden, nicht unnötige Informationen über uns gesammelt werden, die Informationen nur so lange wie nötig aufbewahrt bleiben und wir so möglichst nicht zu gläsernen Bürgerinnen und Bürgern werden. Wir sollen vor Stigmatisierung und Vorurteilen geschützt werden und uns im Rahmen der Privatsphäre frei entfalten können.

In einer Zeit, in der das Sammeln und Verwerten von Personendaten als Wirtschaftsfaktor gilt und bei der Nutzung von digitalen Hilfsmitteln die vollständige Überwachung droht, mit Personendaten gehandelt und versucht wird, alles miteinander zu verknüpfen, um ein noch umfassenderes und damit wertvolleres Bild von einzelnen Personen oder Personengruppen zu erhalten, gilt es ein besonderes Augenmerk auf die Wahrung der Privatsphäre und den Umgang damit zu richten. Die sich rasant entwickelnden technischen Möglichkeiten wie das Speichern von immer grösseren Datenmengen, das Erheben und Erfassen von immer mehr Informationen und immer grössere Verarbeitungsgeschwindigkeiten in Kombination mit «neuen» Bearbeitungsmöglichkeiten wie Künstlicher Intelligenz (KI) müssen sowohl auf ihre Chancen als auch Risiken hin beurteilt werden.

Ob eine freie und sich entwickelnde Gesellschaft, wie wir sie kennen, ohne Privatsphäre überhaupt möglich ist, ist stark zu bezweifeln. Wer ständig überwacht wird oder sich überwacht fühlt, wird versuchen, sein Verhalten so anzupassen, dass er nicht auffällt. Damit ist die freie Entfaltung der Persönlichkeit nicht vereinbar. Autoritäre oder gar totalitäre Systeme waren in der Vergangenheit stets durch einen hohen Grad an Überwachung gekennzeichnet. Eine andere Gefahr besteht darin, dass im privaten Sektor das eigentlich selbstverständliche Gut der Privatsphäre als Zusatznutzen kommerzialisiert wird, indem eine ungehemmte Datenbearbeitung und -bekanntgabe nur durch Bezahlung verhindert werden kann. Die Privatsphäre ist ein kostbares Gut und sollte nicht zu einem Luxus werden, welches sich nur noch ausgewählte Personenkreise leisten können.

1.4 INFORMATIONS- UND DATENSCHUTZGESETZ (IDG)

Unter der Leitung der Sicherheitsdirektion (SID) wird das kantonale IDG überarbeitet (vgl. auch Tätigkeitsberichte 2018 und 2017). Die Revision beschäftigte die ASD auch in diesem Jahr.

Bei der Revision werden die notwendigen und aufgrund des gesellschaftlichen Fortschrittes vor allem auch sinnvollen Anpassungen vorgenommen. Sie wurde angestossen durch die grossen europäischen Datenschutzpakete. Durch ihren Beitritt zum Schengen-Raum ist die Schweiz – und damit auch sämtliche Kantone – verpflichtet, ihre Datenschutzgesetze an die Richtlinie 2016/680 der Europäischen Union für die Datenbearbeitung im Bereich der Strafverfolgung anzupassen. Zudem hat der Bundesrat beschlossen, dem Parlament die modernisierte Datenschutzkonvention 108 des Europarats zur Ratifizierung vorzulegen. Voraussetzung dafür ist ebenfalls die Anpassung der innerstaatlichen Datenschutzgesetze an die Bestimmungen der Konvention. Zusätzlich hat die Schweiz, insbesondere auch die Privatwirtschaft, ein grosses Interesse daran, dass die Neuerungen der DSGVO in vergleichbarer Weise in ihr Recht übertragen werden.

Von der Gleichwertigkeit der innerstaatlichen datenschutzrechtlichen mit den europäischen Bestimmungen hängt die Erneuerung des sogenannten Adäquanzbeschlusses durch die EU ab. Würde die Schweiz diesen Status verlieren, würde der Austausch von Daten mit der EU vertragliche und technische Sicherungsmassnahmen erfordern, was weder im Interesse der Wirtschaft noch der öffentlichen Organe ist.

Da der Gesetzgebungsrahmen, welcher vom europäischen Datenschutzpaket ausgeht, für alle Kantone derselbe ist, erarbeitete eine Expertengruppe der Konferenz der Kantonsregierungen einen Leitfaden, auf welchen sich auch der Kanton Basel-Landschaft bei den Gesetzgebungsarbeiten stützen kann. Zudem steht der Kanton in stetem Austausch mit dem Kanton Basel-Stadt. Diese enge Zusammenarbeit begrüsst die ASD sehr. Die Datenschutzgesetze der beiden Kantone sind bereits heute sehr ähnlich und aufgrund der Zusammenarbeit der beiden Kantone ist es äusserst sinnvoll und erstrebenswert, dass dies auch künftig so bleibt.

Im Kanton Basel-Landschaft werden zudem im Rahmen der Revision zwei hängige Motionen aufgenommen. Zum einen soll die Möglichkeit geschaffen werden, dass Pilotprojekte, bei welchen besondere Personendaten bearbeitet werden, gestützt auf eine Verordnung unter klaren Rahmenbedingungen und für eine beschränkte Zeit durchgeführt werden können. Dies vereinfacht die Durchführung von Pilotprojekten, da der Gesetzgebungsprozess bei einer Gesetzesänderung deutlich länger dauert. Zudem können dann bei der späteren Überführung der rechtlichen Grundlage ins Gesetz die beim Pilot gewonnenen Erkenntnisse einfliessen. Basel-Stadt kennt eine solche Bestimmung bereits und hat gute Erfahrungen damit gemacht. Eine weitere Motion sieht vor, dass Beratungen der ASD für öffentliche Organe ausserhalb der kantonalen Verwaltung kostenpflichtig werden. Der Datenschutzbeauftragte befürchtet, dass dies insgesamt zu einer Schwächung des Datenschutzes in unserem Kanton führt. Der Kanton Basel-Landschaft wäre ausserdem der einzige Kanton in der Schweiz, welcher eine solche Bestimmung kennt.

Zum Ende der Berichtsperiode wurde das kantonsinterne Mitberichtsverfahren abgeschlossen. Nun steht die Vernehmlassung an.

2

AUS DEM BERATUNGSALLTAG

2.1 HERAUSGABE DER ADRESSEN SÄMTLICHER STIMMBERECHTIGTER EINWOHNERINNEN UND EINWOHNER AN EINE POLITISCHE PARTEI

2019 standen turnusgemäss Landrats- sowie National- und Ständeratswahlen an. Viele Parteien wollten gewisse Zielgruppen zusätzlich zum offiziellen Wahlunterlagenversand erreichen, um auf ihre politischen Programme hinzuweisen. Deswegen wurde die ASD mehrfach von verschiedenen Gemeinden angefragt, ob eine Bekanntgabe der Adressdaten aus dem Einwohnerregister für den Versand von Wahlunterlagen politischer Parteien zulässig sei.

Die ASD konnte den Gemeinden mitteilen, dass dieses Vorgehen eine Bekanntgabe zu einem schützenswerten ideellen Zweck im Sinne von § 3 Abs. 3 des kantonalen Anmeldungs- und Registergesetzes (ARG) darstelle und daher zulässig sei. Bei einer solchen Listenbekanntgabe sind die anfragenden Personen von der Gemeinde jeweils zu verpflichten, die Adressen nur für diesen Zweck zu verwenden und diese auch nicht an Dritte weiterzugeben. Gesperrte Daten dürfen zudem nicht bekanntgegeben werden.

2.2 ZUGANGSGESUCH ZU EINER NICHT VORHANDENEN STATISTIK BEI EINER BEHÖRDE UND DER ANSPRUCH AUF EINE ANFECHTBARE VERFÜGUNG

Eine Person verlangte von einer kantonalen Behörde die Herausgabe einer Statistik betreffend ein für sie relevantes Thema. Das öffentliche Organ teilte der gesuchstellenden Person mit, dass es entsprechende Daten nicht erhoben habe, da zu wenige Fälle existierten und eine entsprechende Statistik deshalb auch keine Aussagekraft hätte. Die Behörde gelangte daraufhin an die ASD und wollte von dieser einerseits wissen, ob sie die verlangte Statistik erstellen und im Rahmen des Zugangsgesuchs bekanntgeben müsse und ob, falls dies nicht der Fall sei und die Behörde eine Abweisung des Zugangsgesuchs in Betracht ziehe, die um Zugang ersuchende Person Anspruch auf eine anfechtbare Verfügung habe.

Die ASD konnte der anfragenden Behörde gegenüber ausführen, dass gemäss § 23 IDG jede Person Anspruch auf Zugang zu Informationen hat, die bei den öffentlichen Organen vorhanden sind. Aus der Legaldefinition des Begriffes «Information» gemäss § 3 Abs. 2 IDG ergibt sich, dass die Information in einer beliebigen Darstellungsform existieren bzw. auf einem beliebigen Informationsträger aufgezeichnet sein kann, um als vorhanden im Sinne von § 23 IDG zu gelten. Ist eine Information demnach in elektronischer Form vorhanden, muss sie – stets unter dem Vorbehalt der Prüfung von Verweigerungs- und Einschränkungsgründen gemäss § 27 IDG – der gesuchstellenden Person in geeigneter Form ausgehändigt werden. Wenn ein Zugangsgesuch eine Information zum Gegenstand hat, die nicht direkt vorhanden, aber mittels eines einfachen elektronischen Verfahrens, sozusagen «auf Knopfdruck» (z. B. durch Zusammenziehen verschiedener Werte) erstellt werden kann, so ist das öffentliche Organ verpflichtet, dies zu tun. Allerdings ist es nicht verpflichtet, neue Verknüpfungen vorzunehmen und Informationen aus verschiedenen Quellen zusammenzusuchen. Nicht relevant ist dabei ganz grundsätzlich, wie aussagekräftig die herausverlangten Informationen sind. Diesbezüglich besteht der Zugangsanspruch voraussetzungslos. Schliesslich gilt beim Herausverlangen einer Statistik vom öffentlichen Organ stets auch zu berücksichtigen, dass die zugangsstellende Person anstelle der Statistik ebenso Zugang zu den einzelnen Rohdaten, mit welcher die Statistik erstellt würde, verlangen und sich so dann die Statistik selbst erstellen könnte.

Ein angefragtes öffentliches Organ hat zusammenfassend jeweils im konkreten Einzelfall zu prüfen und zu entscheiden, ob Informationen vorhanden sind bzw. ob diese leicht erstellt werden können und ob Einschränkungsgründe im Sinne von § 27 IDG vorliegen. Kommt es am Ende seiner Prüfung zum Schluss, dass es den Zugang zu den Informationen verweigern muss, hat es dies der zugangsgesuchstellenden Person mitzuteilen. Diese kann anschliessend innert 30 Tagen vom öffentlichen Organ eine anfechtbare Verfügung verlangen.

2.3 HERAUSGABE VON UNTERLAGEN EINES FALLES DURCH DIE KOMMUNALE SOZIALHILFEBEHÖRDE AN DEN FACHVERBAND SKOS

Das kantonale Sozialamt (SVA) gelangte mit folgendem Sachverhalt an die ASD: Die Schweizerische Konferenz für Sozialhilfe (SKOS) bietet als Fachverband seinen Mitgliedern, zu denen verschiedene Bundesämter, sämtliche Kantone und viele Gemeinden gehören, unter anderem Beratungen in komplexen Fällen an. Die SVA fragte nach,

ob kommunale Sozialhilfebehörden dem Verband im Rahmen einer konkreten Beratung Unterlagen mit Personendaten aus einem laufenden Fall zukommen lassen dürften oder ob ein solches Vorgehen der in § 38 des kantonalen Sozialhilfegesetzes (SHG) statuierten Schweigepflicht widersprechen würde.

Die ASD konnte dem SVA mitteilen, dass die kommunalen Sozialhilfebehörden die Fälle der SKOS wenn immer möglich in anonymisierter Form schildern sollten. Bei anonymisierten Daten stellen sich keine datenschutzrechtlichen Fragen und das IDG ist nicht anwendbar. Falls dies nicht möglich ist, muss Folgendes beachtet werden: Wenn kommunale Sozialhilfebehörden dem Verband konkrete Fälle mit nicht anonymisierten Daten schildern, geben sie diesem regelmässig Personendaten bekannt, welche der Verband dann im Rahmen seiner Beratungstätigkeit bearbeitet. Nach § 7 Abs. 1 IDG kann ein öffentliches Organ das Bearbeiten von Informationen Dritten übertragen, wenn keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und gleichzeitig sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte. Darüber hinaus bleibt das öffentliche Organ nach § 7 Abs. 2 IDG für den Umgang mit Informationen nach dem IDG verantwortlich. Eine kommunale Sozialhilfebehörde muss somit die Einhaltung der Voraussetzungen von § 7 IDG sicherstellen. Dies hat einerseits vertraglich zu erfolgen. Andererseits hat sie die erforderlichen organisatorischen und technischen Massnahmen zu ergreifen bzw. sicherzustellen, dass entsprechende Massnahmen vom beauftragten Dritten ergriffen werden, um die Personendaten vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen.

2.4 GEBÜHRENERHEBUNG BEI GESUCHEN UM ZUGANG ZU INFORMATIONEN DURCH MEDIENSCHAFFENDE

Eine Behörde gelangte an die ASD, weil sie bei der Beurteilung eines Zugangsgesuchs eine Frage betreffend die Erhebung von Gebühren in aufwendigen Verfahren gemäss § 34 IDG hatte. Die Behörde habe der gesuchstellenden Person vorab eröffnet, dass das Zugangsgesuch mit Gebühren verbunden wäre, weil sie einen bestimmten Aufwand bei der Zusammenstellung der Informationen betreiben müsse. Daraufhin habe sich die gesuchstellende Person gemeldet und gemeint, dass ein Nachbarskanton bei Medienschaffenden auf eine Gebührenerhebung verzichte. Das sei dort gängige Praxis. Das öffentliche Organ wollte von der ASD wissen, ob dies korrekt sei und ob im Kanton Basel-Landschaft eine ähnliche Praxis bestehe.

Die ASD konnte der Behörde mitteilen, dass ihr die Praxis im Nachbarskanton nicht bekannt sei und im Kanton Basel-Landschaft wider besseres Wissen keine entsprechende Praxis bestehe. Das IDG i. V. m. der Informations- und Datenschutzverordnung (IDV) sieht freilich eine zeitliche Vorzugsbehandlung von Medienschaffenden vor, soweit dies möglich ist. Die ASD teilt zudem die Meinung in der Lehre, dass in solchen Fällen i. d. R. keine Gebühr erhoben werden soll, weil ja eben kein grosser Aufwand betrieben wurde. Ein Anspruch auf Kostenlosigkeit besteht jedoch für Medienschaffende nicht, was auch schon das Bundesverwaltungsgericht in einem Entscheid bestätigt hat. Bei einem aufwendigen Verfahren kann gemäss § 34 IDG auch Medienschaffenden eine angemessene Gebühr auferlegt werden.

2.5 KALENDERFREIGABE GEGENÜBER EINER VORGESETZTEN PERSON

Eine beim Kanton angestellte Person meldete sich bei der ASD, weil ihre vorgesetzte Person eine umfassende Outlook-Kalenderfreigabe verlangte, um uneingeschränkten Einblick in sämtliche Einträge zu erhalten. Die anfragende Person machte sich Sorgen, weil ihre Termine im Kalender detaillierte und zum Teil sehr heikle Angaben zu den von ihr bearbeiteten Fällen enthielten. Da sie einer Geheimhaltungspflicht unterstehe, fragte sie sich, wie weit diese gehe und ob eine völlige Freigabe gegenüber ihrer vorgesetzten Person aus datenschutzrechtlicher Sicht zulässig sei.

Die ASD konnte der anfragenden Person gegenüber ausführen, dass aus arbeitsrechtlicher Sicht die vorgesetzte Person eine Leitungs- und Aufsichtsfunktion innehat. Gestützt darauf ist sie grundsätzlich berechtigt, zu erfahren, welche Fälle bearbeitet werden und sich so z. B. darüber zu informieren, wo und in welcher Tätigkeit die Mitarbeitenden unterwegs sind. Die vorgesetzte Person selbst untersteht auch der Schweigepflicht. Deshalb ist es aus datenschutzrechtlicher Sicht grundsätzlich zulässig, dass sie Einblick in die Angaben zu den Fällen erhält, selbst dann, wenn diese heikle Daten enthalten. Allerdings müssen, wie

im öffentlich-rechtlichen Bereich immer, die allgemeinen Grundsätze der Notwendigkeit bzw. der Verhältnismässigkeit berücksichtigt werden. Dabei kommt der Grösse und Struktur einer Organisation eine wichtige Bedeutung zu. Mitarbeitende können immer auch mit Initialen oder Fallnummern arbeiten, womit sie die Bekanntgabe von Informationen im Kalender in einem gewissen Mass steuern, weil so auf den ersten Blick z. B. nicht unmittelbar ersichtlich wird, mit wem und in welchem Zusammenhang ein Termin vereinbart wurde.

Die ASD konnte der anfragenden Person ausserdem mitteilen, dass eine vorgesetzte Person keine Einsicht in private Termine ihrer Mitarbeitenden verlangen darf. Solche Termine können von diesen im Outlook-Kalender als «privat» markiert werden und sind dann von niemandem ausser der Person selbst einsehbar.

2.6 AUTOMATISCHE WEITERLEITUNG EINER EINGEHENDEN MAIL VON EINER GESCHÄFTLICHEN AN EINE PRIVATE MAILADRESSE

Eine bei einem öffentlichen Organ angestellte Person wollte von der ASD wissen, ob eine automatische Weiterleitung von Mails, welche an die geschäftliche Adresse von Angestellten des öffentlichen Organs gingen, an deren private Mailadresse erlaubt sei. Zudem erkundigte sich die anfragende Person, ob die Nutzung einer beruflichen Mailadresse durch Angestellte zwingend sei oder ob Angestellte bei der Arbeit auch eine private Mailadresse verwenden dürften.

Die ASD machte die anfragende Person darauf aufmerksam, dass aus Transparenzgründen sowie aus Gründen der Informationssicherheit auf eine automatische Weiterleitung von auf eine Geschäftsadresse eingehenden Mails an eine private Mailadresse verzichtet werden sollte. Die Absenderin geht beim Versand zu Recht davon aus, dass ihre Mail auch tatsächlich der gewählten Geschäftsmailadresse zugestellt wird. Öffentliche Organe müssen ihre Informationen gemäss § 8 IDG durch angemessene technische und organisatorische Massnahmen u. a. auch vor unrechtmässiger Kenntnisnahme schützen. Bei einer Weiterleitung an eine private Mailadresse würden diese Massnahmen nicht mehr greifen. Je nach privatem E-Mail-Provider wird dieser gar ermächtigt, die Informationen weiterzuverwenden. Empfehlenswert ist in diesem Zusammenhang die Aufstellung von Richtlinien durch die Organisation, z. B. in einem internen Reglement, welches den Umgang bzw. die Benutzung von Informatikmitteln festlegt. Aus den gleichen Überlegungen sollte, wenn immer möglich, eine ordentliche Geschäftsmailadresse verwendet werden – auch von Angestellten, welche in einem Kleinpensum tätig sind.

2.7 UMFANG DES EINSICHTSRECHTS VON PATIENTINNEN UND PATIENTEN DER PSYCHIATRIE BASELLAND IN IHRE DOSSIERS

Die Psychiatrie Baselland gelangte an die ASD, weil Patientinnen und Patienten immer wieder Einsicht in ihre Dossiers verlangen. Letztere würden regelmässig auch Berichte von anderen Spitälern und externen Ärzten enthalten oder auch solche, welche die Psychiatrie z. B. zuhanden von Versicherungen erstellt. Der Psychiatrie Baselland stelle sich in diesem Zusammenhang die Frage, ob die Patientinnen und Patienten diese Berichte bei ihnen einsehen und herausverlangen könnten oder ob sie die anfragenden Personen an die externen Stellen verweisen dürfe.

Die ASD konnte der Psychiatrie Baselland aufzeigen, dass bei der vorliegend verlangten Einsicht in das eigene Patientendossier die Voraussetzungen des Rechts auf Zugang zu den eigenen Personendaten gemäss § 24 IDG geprüft werden müssen. Nach dieser Bestimmung hat jede Person Anspruch auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen, ausgenommen zu Aufzeichnungen, welche nicht fertiggestellt sind. Darüber hinaus enthält auch das kantonale Gesundheitsgesetz (GesG) in § 44 Abs. 1 eine explizite Regelung zum Einsichtsrecht in die eigene Patientendokumentation. Gemäss dieser Bestimmung hat die Patientin bzw. der Patient das Recht, die gesamte sie bzw. ihn betreffende Patientendokumentation einzusehen. Bei beiden Rechten handelt es sich grundsätzlich um ein umfassendes Einsichtsrecht. Dies bedeutet, dass auch Berichte, Korrespondenzen und Überweisungsschreiben von Dritten Teil des Patientendossiers sind und eingesehen werden dürfen. Aus dem Patientendossier muss zudem ersichtlich sein, wer welche Einträge verfasst hat. Werden Informationen festgehalten, die von Dritten stammen, ist dies entsprechend anzugeben. Das Einsichtsrecht kann jedoch gemäss § 27 Abs. 1 IDG teilweise oder ganz eingeschränkt werden, wenn überwiegende öffentliche

oder private Interessen entgegenstehen. Dies kann zum Beispiel dann der Fall sein, wenn gewisse Informationen in einem Patientendossier von Angehörigen stammen, die nicht möchten, dass der Patient bzw. die Patientin davon erfährt. Die ASD konnte der Psychiatrie Baselland aufzeigen, dass sie als angefragtes öffentliches Organ verpflichtet ist, im konkreten Einzelfall die Interessensabwägung vorzunehmen. Ein weiterer Einschränkungsgrund findet sich in § 27 Abs. 4 IDG: Ist es wegen der Interessen der um Zugang ersuchenden Person erforderlich, kann der Zugang zur eigenen Patientendokumentation auch eingeschränkt werden.

2.8 HANDHABUNG DER ABZUGSFÄHIGKEIT VON GESUNDHEITSKOSTEN DURCH DIE STEUERVERWALTUNG, WENN DIE LEISTUNGSERBRINGER AUF DER LEISTUNGSBESCHEINIGUNG DER KRANKENKASSE VON DER DEKLARIERENDEN PERSON EINGESCHWÄRZT WURDEN

Eine Privatperson wandte sich an die ASD. Sie erhalte jedes Jahr von der Krankenversicherung eine Leistungsübersicht der Krankheitskosten für die Steuererklärung. Auf der detaillierten Leistungsübersicht seien jeweils die bezogenen Leistungen und die Leistungserbringer erkennbar. Die Person wollte von der ASD wissen, ob sie der Steuerverwaltung wirklich sämtliche Informationen bekanntgeben müsse oder ob sie zumindest die Leistungserbringer einschwärzen könne, damit sie vor der Steuerverwaltung nicht offenlegen müsse, bei welchem Arzt bzw. bei welcher Ärztin oder in welcher Klinik sie sich behandeln liess.

Die ASD konnte der Person gegenüber darlegen, dass sich die kantonale Steuerverwaltung auf eine gesetzliche Grundlage, nämlich das Steuergesetz, stützen kann, um Informationen zur Beurteilung der Rechtmässigkeit von geltend gemachten Abzügen zu erheben. Die Steuerverwaltung ist dabei aber an das Verhältnismässigkeitsprinzip gebunden. Die Informationen müssen gemäss § 9 Abs. 1 IDG zur Beurteilung erforderlich sein, damit sie von der Steuerverwaltung erhoben werden dürfen.

Bei den Krankheitskosten ist zwischen selbstgetragenen und nicht versicherten Kosten zu unterscheiden. Selbstgetragene Kosten sind grundsätzlich versicherte Kosten im Sinne des bundesrechtlichen Krankenversicherungsgesetzes, welche aber nicht von den Krankenversicherungen übernommen, sondern von den Versicherten selbst getragen werden (z. B. der Selbstbehalt). Diese Kosten wurden bereits durch die Krankenversicherung beurteilt. Somit handelt es sich per se um abzugsfähige Kosten, weshalb bei diesen die Notwendigkeit zur Erhebung von Detailinformationen nicht gegeben ist und sie auf der Leistungsbescheinigung eingeschwärzt werden dürfen. Bei den nicht versicherten Kosten hatte die Krankenversicherung lediglich geprüft, ob Kosten versichert seien, und kam zu einem negativen Ergebnis. Entsprechend müssen diese Kosten durch die Steuerverwaltung auf ihre Abzugsfähigkeit hin geprüft werden können. Dazu ist regelmässig die Erhebung von Detailinformationen erforderlich. Aber auch hier gilt, dass Informationen, die eindeutig nicht für die Beurteilung notwendig sind, eingeschwärzt werden können.

2.9 BEKANNTGABE VON PERSONENDATEN AN DIE LANDESKIRCHEN

Verschiedentlich stellte sich in der Beratungstätigkeit der ASD die Frage, ob und inwieweit die Landeskirchen Daten über Personen bearbeiten dürfen, die nicht ihrer Konfession angehören. Für die Durchführung ihrer Aufgaben sowie zur Erhebung der Kirchensteuer ist es ohne Frage erforderlich, dass die Kirchen Zugriff auf die Informationen ihrer eigenen Mitglieder haben müssen. Bei Personen, die nicht der jeweiligen Kirche angehören, ist die Frage heikler, nicht zuletzt darum, da es sich bei Informationen zur Religionszugehörigkeit um besondere Personendaten handelt, die eines höheren Schutzes bedürfen. Die Regeln sind dabei die gleichen wie immer. Entweder es ist eine ausdrückliche gesetzliche Grundlage vorhanden oder das Bearbeiten der Daten ist für die Erfüllung der gesetzlichen Aufgabe erforderlich. Ferner ist zu unterscheiden, ob der Datenfluss automatisch erfolgt, also ob die Kirchen ohne ihr Zutun Meldungen über Nichtmitglieder erhalten oder sogar Zugriff auf eine Datenbank haben oder ob sie die Informationen im Einzelfall auf Anfrage beziehen.

Die Vertreterinnen und Vertreter der Landeskirchen konnten aufzeigen, dass es in gewissen Fällen für die seelsorgerische Betreuung notwendig sein kann, die Religionszugehörigkeit des Partners oder der Partnerin zu kennen. Diese Art der Begründung könnte den Anspruch auf eine Kenntnis der Daten im Einzelfall begründen. Auch für die Erhebung der Kirchensteuer ist die Kenntnis der Konfession des im

gleichen Haushalt lebenden Ehepartners von Bedeutung, da bei gemischten Haushalten die Kirchensteuer anteilsmässig erhoben wird. Genau genommen müsste daher nur bekanntgegeben werden, ob die Person die gleiche Religionszugehörigkeit hat wie der Partner bzw. die Partnerin.

Im Übrigen ist darauf hinzuweisen, dass eine Bekanntgabe der Konfession durch die Einwohnergemeinden gestützt auf die Daten des Einwohnerregisters ohnehin nur in beschränktem Masse möglich ist, da das entsprechende Registerfeld «Konfessionszugehörigkeit» nur die Ausprägungen der drei kantonal anerkannten Landeskirchen plus «unbekannt» enthält. Ist eine Person z. B. jüdischen Glaubens, Angehörige der Zeugen Jehovas oder konfessionslos, so ist diese Tatsache den Gemeinden unbekannt und kann folglich auch nicht bekanntgegeben werden.

Zusammenfassend kann gesagt werden, dass die Landeskirchen (ausschliesslich) zur Durchführung der Steuererhebung sowie im Einzelfall zur seelsorgerischen Tätigkeit Anspruch haben auf die Kenntnis der eingetragenen Konfessionszugehörigkeit von Personen, die ihnen nicht angehören.

2.10 ZESSION VON STEUERFORDERUNGEN

Vonseiten der Gemeinden wurde die Frage aufgeworfen, wie eine allfällige Zession einer Steuerforderung datenschutzrechtlich zu beurteilen sei.

Bei einer Zession findet vereinfacht gesagt eine Abtretung einer Forderung an einen anderen Gläubiger statt. Eine solche Abtretung kann ohne Zustimmung des Schuldners geschehen. Der ehemalige Gläubiger ist gesetzlich verpflichtet, dem neuen Gläubiger sämtliche Beweise auszuhändigen, die es diesem ermöglichen, die Forderung geltend zu machen. Somit ist bei einer Zession immer ein Informationsfluss vorgesehen, womit sich auch datenschutzrechtliche Fragen stellen. Bei einer Zession einer Steuerforderung müssten demnach regelmässig Steuerdaten fliessen, im Minimum aber die rechtskräftige Steuerveranlagung übermittelt werden.

Allerdings ist eine Zession nicht in allen Fällen zulässig. Gemäss Art. 164 Abs. 1 OR ist eine Zession zulässig, «soweit nicht Gesetz, Vereinbarung oder die Natur des Rechtsverhältnisses entgegenstehen». Das Bundesverwaltungsgericht hat in einem Entscheid festgehalten, dass die Abtretung einer dem Staat zustehenden Steuerforderung generell nicht zulässig sei. Das Gemeinwesen trete mit hoheitlicher Gewalt auf, um die Einnahmen zur Bestreitung seiner laufenden Ausgaben zu generieren. Damit stünde der beschriebenen Abtretung schon die Natur des Rechtsverhältnisses entgegen (Urteil A-4007/2016 des Bundesverwaltungsgerichts vom 18. Mai 2018, Erwägung 7.5.2.3).

Damit ist auch die datenschutzrechtliche Frage entschieden. Denn aufgrund des Legalitätsprinzips, welches für den Datenschutz in § 9 IDG verankert ist, muss jede Bearbeitung von Personendaten durch öffentliche Organe auf einer gesetzlichen Grundlage beruhen. Im Normalfall sind solche Bestimmungen im Sachrecht zu finden und erlauben eine Datenbearbeitung zur Erfüllung einer öffentlichen Aufgabe. Vorliegend haben wir es aber mit einer Bestimmung zu tun, die eine staatliche Tätigkeit, die Zession von Steuerforderungen, untersagt. In der Folge ist aber auch die damit notwendigerweise verbundene Bekanntgabe von Personendaten nicht erlaubt. Eine Zession von Steuerforderungen erweist sich deshalb auch datenschutzrechtlich als unzulässig.

Die Aufsichtsstelle hatte in einer früheren Berichtsperiode die Frage zu prüfen, ob die Bewirtschaftung von Verlustscheinen durch ein Inkassobüro im Auftrag eines öffentlichen Organs rechtmässig sei. Die Aufsichtsstelle hatte dabei festgehalten, dass dies keine Zession darstelle und den Vorgang als ein Bearbeiten im Auftrag im Sinne von § 7 IDG qualifiziert. Dies ist zulässig, immer unter Beachtung der entsprechenden Bestimmungen betreffend Verantwortung und (vertragliche) Sicherstellung der Einhaltung der datenschutzrechtlichen Vorgaben durch den Auftragnehmer. So dürfen die bekanntgegebenen Informationen vom Auftragnehmer auch nicht für andere Zwecke, wie beispielsweise für eine Bonitätsprüfung, verwendet werden. Ein weiterer Unterschied besteht darin, dass für die Bewirtschaftung des Verlustscheins keine weiteren Informationen über die betroffene Person erforderlich sind, da der Verlustschein als Schuldanerkennung dient.

2.11 DARF DER GEMEINDERAT DIE ERRICHTUNG EINER VIDEOÜBERWACHUNGSANLAGE BESCHLIESSEN?

Eine Gemeinde erkundigte sich bei der Aufsichtsstelle, ob es in der Kompetenz des Gemeinderats liege, eine Videoüberwachungskamera im öffentlichen Raum zu installieren, oder ob dazu die Zustimmung der Gemeindeversammlung erforderlich sei.

Die personenbezogene Überwachung des öffentlichen Raums ist ein nicht unerheblicher Eingriff in die Grundrechte der betroffenen Personen. Wie bei jeder Bearbeitung von Personendaten braucht es dazu eine gesetzliche Grundlage. Diese muss über eine allgemeine Ermächtigung zur Installation von Kameras hinausgehen und möglichst präzise die Voraussetzungen und Rahmenbedingungen regeln. Bestimmt werden typischerweise die zur Installation berechtigten öffentlichen Organe, erlaubte Zwecke der Überwachung, Regeln betreffend die Weitergabe der Aufzeichnungen, Aufbewahrungsfristen etc.

Die Regelung der personenbezogenen Überwachung des öffentlichen Raums ist seit dem 1. Januar 2015 in Kraft. Verankert wurde sie in § 45d ff. des Polizeigesetzes (PolG). Danach sind nicht nur die Kantonspolizei, sondern auch diverse andere öffentliche Organe wie etwa die Gemeinden befugt, Videoüberwachungen «anzuordnen». Diese müssen die Anforderungen der Bestimmungen im Polizeigesetz erfüllen. Zentral ist dabei die Pflicht zum Erlass eines Betriebsreglements. Das Polizeigesetz schreibt relativ detailliert vor, welche Punkte darin zu regeln sind. Die ASD hat zudem auf ihrer Webseite ein Merkblatt, ein Musterreglement sowie Erläuterungen aufgeschaltet.

Für Missverständnisse sorgt in der Praxis manchmal die Bezeichnung «Betriebsreglement». In den Gemeinden sind Reglemente formelle Gesetze, die von der Gemeindeversammlung beschlossen werden müssen. Darum handelt es sich beim Betriebsreglement jedoch nicht. Zuständig für den Erlass dieser Regelungen, die man beispielsweise auch als «Betriebsordnung» bezeichnen könnte, ist das jeweilige öffentliche Organ, welches die Videoüberwachung anordnet. Dies kann jeder der in § 45d Abs. 1 Polizeigesetz genannten sein. In einer Gemeinde ist in der Regel der Gemeinderat für den Erlass zuständig.

Die ASD konnte somit der Gemeinde bestätigen, dass die Videoüberwachung nicht von der Gemeindeversammlung beschlossen werden muss, da im Polizeigesetz auch für die Gemeinden eine ausdrückliche, formellgesetzliche Grundlage besteht. Allerdings muss der Gemeinderat das Betriebsreglement erlassen. Anders als in anderen Kantonen muss eine Videoüberwachung im Kanton Basel-Landschaft nicht bei der ASD angemeldet oder von ihr genehmigt werden, jedoch steht sie bei Fragen beratend zur Verfügung. Zudem kann sie die Einhaltung der Bestimmungen im Rahmen ihrer regulären Kontrolltätigkeit überprüfen.

2.12 RECHERCHE VON STRAFTÄTERN BZW. STRAFTÄTERINNEN IM PERSONENREGISTER

Ein Gemeindeverwalter gelangte mit folgender Fragestellung an die Aufsichtsstelle: Bei einem Schulhaus war eine Wand beschmiert worden. Einer der Mittäter war dem Gemeindeverwalter bekannt. Zur Rede gestellt, gab der Missetäter preis, wer sonst noch beteiligt gewesen sei. Ihm waren allerdings nur die Vornamen der Kollegen bekannt. Da alle Beteiligten jedoch in derselben Gemeinde wohnten, wäre es möglich gewesen, die Identitäten über eine Abfrage im kantonalen Personenregister arbo zu ermitteln. Der Gemeindeverwalter wollte abklären, ob dieses Vorgehen rechtlich möglich sei.

Der Kanton Basel-Landschaft führt unter der Bezeichnung arbo ein kantonales Personenregister. Der Inhalt des Registers, der Verwendungszweck sowie die Regelung der Zugriffe richten sich nach dem Anmelde- und Registergesetz und seiner Verordnung. Etwas vereinfacht gesagt enthält arbo sämtliche Personenregisterdaten von Personen, die im Kanton Basel-Landschaft niedergelassen sind oder eine Aufenthaltsbewilligung haben. Zusätzlich werden verschiedene Merkmale von natürlichen und juristischen Personen erfasst, die im Kanton Grundeigentum besitzen. Der Zweck dieses zentralen Registers ist u. a. die Bereitstellung aktueller Daten für öffentliche Organe, sowohl zur Unterstützung im Tagesgeschäft als auch im Ereignisfall. Der Kreis der öffentlichen Organe, welche Zugriff auf arbo haben können, ist ebenfalls im Gesetz festgelegt. Die Gemeinden sind darin selbstverständlich auch enthalten. In der Anmelde- und Registerverordnung wird das Verfahren beschrieben, mittels welchem ein im Gesetz aufgeführtes öffentliches Organ

auf arbo zugreifen kann. In Anhang II der Verordnung sind zudem die konkreten Zugriffsrechte der einzelnen öffentlichen Organe aufgeführt. Der Umfang der Berechtigung eines öffentlichen Organs soll dabei möglichst genau seinen Aufgaben entsprechen; für deren Erfüllung nicht notwendige Merkmale werden nicht freigeschaltet. Entsprechend steht auch in der konkreten Anwendung, d. h. dem Bezug von Personendaten über arbo, stets die zu erfüllende Aufgabe im Zentrum. Für andere Zwecke darf ein öffentliches Organ keine Daten aus arbo beziehen, auch wenn dies technisch aufgrund der vergebenen Rechte möglich wäre.

Damit hat das kantonale Personenregister arbo eine umfassende Regelung erfahren, welche in vieler Hinsicht vorbildlich ist für grosse Datenbestände, die einem weiten Kreis von öffentlichen Organen für ihre Zweckerfüllung zur Verfügung stehen. Die Frage, ob ein öffentliches Organ ein bestimmtes Registermerkmal einer Person bearbeiten darf, wird somit soweit möglich generell-abstrakt geregelt.

Für den Fall der beschmierten Wand galt es demnach zu prüfen, ob die Ermittlung der Täter bzw. Täterinnen Teil der Aufgaben des Gemeindeverwalters ist. Die Prüfung der entsprechenden gesetzlichen Grundlagen auf kantonaler und kommunaler Ebene ergab in diesem Fall, dass die Ermittlung der Täterschaft nicht Aufgabe des Verwalters, sondern der (Gemeinde-)Polizei ist. Damit waren die Voraussetzungen für die Recherche des Gemeindeverwalters in arbo nicht gegeben.

2.13 ERKENNBARKEIT DER MAIL-ADRESSEN SÄMTLICHER EMPFÄNGER BEIM VERSAND EINER MAIL

Die ASD wurde von einer Privatperson darauf aufmerksam gemacht, dass ein öffentliches Organ der kantonalen Verwaltung Mails, welche an eine Mehrzahl von Empfängern versendet wurden, regelmässig so versende, dass ihre Mail-Adressen für alle ersichtlich seien.

Die ASD konnte der anfragenden Person das korrekte Vorgehen für öffentliche Organe beim Versand von Mails an eine Mehrzahl von Empfängern erläutern. Werden die Mail-Adressen im üblichen Adressfeld eingefügt, sind diese für alle sichtbar. Bei einem solchen Versand werden in unzulässiger Weise Personendaten bekanntgegeben, da weder eine gesetzliche Grundlage existiert, welche ein solches Vorgehen erlaubt, noch die entsprechende Bekanntgabe zur Aufgabenerfüllung erforderlich ist. Eine solche unerlaubte Bekanntgabe kann verhindert werden, indem der Absender im ersten Adressfeld seine eigene Mail-Adresse einfügt und die Mail-Adressen sämtlicher Empfänger in das Feld «blinde Kopie» (Bcc) aufnimmt. So erhalten alle Empfänger die Nachricht, ohne die Mail-Adressen der anderen Empfänger sehen zu können.

3

VORABKONTROLLE

Die Vorabkontrolle wurde im Jahre 2008 als präventives Instrument gesetzlich verankert, um eine geplante Personendatenbearbeitung durch öffentliche Organe rechtzeitig auf ihre Vereinbarkeit mit rechtlichen, organisatorischen und technischen Anforderungen an Datenschutz und Informationssicherheit zu prüfen. Mit der Vorabkontrolle wird geprüft, ob das für die Datenbearbeitung zuständige öffentliche Organ die Informationen auf der Basis einer ausreichenden Rechtsgrundlage und mit angemessenen organisatorischen und technischen Schutzmassnahmen bearbeiten wird. So kann ein entsprechendes Risiko bereits während des Projektes und vor der Tätigung grosser Investitionen eingeschätzt und mit geeigneten Massnahmen reduziert werden. Basierend auf den Ergebnissen aus der Projektabwicklung nimmt die ASD eine unabhängige Risikoeinschätzung vor und entscheidet mittels einer Vorprüfung (Triage), ob sie eine Vorabkontrolle durchführt und wie umfangreich und detailliert diese ggf. ausfällt. Die dafür verwendeten Grundlagen müssen für Projekte unabhängig von einer allfälligen Vorabkontrolle erarbeitet werden. Sie sind wesentliche Bestandteile eines geordneten Projektmanagements und werden im Laufe eines Informatikprojektes im Interesse eines rechtmässigen, sicheren und zuverlässigen Betriebs ohnehin erarbeitet.

Die Vorabkontrolle selbst trägt zu einer nachhaltigen und wirtschaftlichen Umsetzung des Datenschutzes und der Informationssicherheit im Allgemeinen bei. Sie findet im Gegensatz zur Kontrolle vor der geplanten Datenbearbeitung statt, d. h. vor und während der Konzeption, auf jeden Fall aber noch vor dem Abschluss der Konzeptphase. So können die konkreten Anforderungen im Bereich des Datenschutzes rechtzeitig berücksichtigt und aufwendige Nachbesserungen bei oder nach der Realisierung und Einführung vermieden werden. Angesichts der rasch zunehmenden Digitalisierung wird es immer wichtiger, dass Datenschutzanforderungen bereits frühzeitig aufgenommen und berücksichtigt werden können. Mit der Vorabkontrolle bzw. dem Ergebnis daraus kann so der Aufwand für eine datenschutzkonforme und ausreichend sichere Lösung verringert und insgesamt ein Effizienzgewinn erzielt werden. Abgesehen von der Vermeidung von datenschutzrechtlichen und informationssicherheitsrelevanten Risiken kann die Vorabkontrolle einen weitergehenden Projektnutzen bringen. Sie ist gerade bei grösseren Projekten ein Prozess, der das Projekt begleitet, dessen Dauer somit auch vom jeweiligen Projektplan abhängig ist. Dies bedeutet, dass keine umfassende Prüfung aller für das Projekt relevanten Aspekte zu einem einzigen Zeitpunkt und mit entsprechendem Zeitaufwand stattfindet. Vielmehr erfolgt die Prüfung in mehreren Teilschritten, wobei in jedem Teilschritt nur die in dieser Projektphase anfallenden Ergebnisse geprüft werden. Die Anzahl der Teilschritte sowie Umfang und Tiefe der Prüfung sind u. a. abhängig von der Art des Projektes, seiner Komplexität, seiner Verbreitung sowie der Anzahl der Benutzer. Dieses Vorgehen hat mehrere Vorteile. Einerseits erfolgt die Teilprüfung direkt nach Vorliegen einzelner Ergebnisse, d. h. das Projekt kann danach in der entsprechenden Projektphase fortgesetzt werden, und andererseits ist der Zeitaufwand für den jeweiligen Prüfungsschritt erheblich geringer, sodass die Teilprüfungen in aller Regel innerhalb von wenigen Wochen vorgenommen werden können. Dadurch wird die Gefahr einer längeren Verzögerung des Projektes minimiert.

Der Aufsichtsstelle Datenschutz ist es ein Anliegen, dass ihre Empfehlungen in der Praxis umsetzbar und den öffentlichen Organen und Benutzern zumutbar sind. Damit die Anforderungen des Datenschutzes inklusive der Informationssicherheit zusammen mit anderen Anforderungen, wie etwa jenen an die Benutzerfreundlichkeit, berücksichtigt werden können, ist es deshalb notwendig, diese rechtzeitig mitzudenken und mitzukonzipieren. Mit Hilfe von «bewährten Praktiken» oder Standards lassen sich meist verschiedene Massnahmen definieren, mit welchen – einzeln oder kombiniert – ein ausreichendes Sicherheitsniveau erreicht werden kann. In jedem Fall bleibt die Informationseignerin, d. h. das öffentliche Organ, welches die Daten für die Erfüllung seiner gesetzlichen Aufgabe bearbeitet, dafür verantwortlich, dass Informationen ausreichend geschützt werden.

Bei zehn von den im Berichtsjahr insgesamt 32 eingegangenen Projekten entschied die Aufsichtsstelle, keine Vorabkontrolle durchzuführen. Die jeweilige Vorprüfung auf der Basis der abgegebenen Dokumentation ergab, dass die Datenbearbeitung entweder keine besonderen Risiken für die betroffenen Personen mit sich brachte oder die Risiken weniger hoch zu gewichten waren als bei anderen, im selben Zeitraum eingereichten Projekten, und deshalb nicht geprüft werden konnten. Drei Projekte wurden zu spät im Projektablauf vorgelegt, weshalb unsere Empfehlungen im Projekt keine Wirkung mehr hätten entfalten können.

Die Aufsichtsstelle verfasste im Berichtsjahr 25 Stellungnahmen zu verschiedenen Projekten. Schwerpunktmässig zeigte sich wie schon in den Vorjahren bei den vorab geprüften Vorhaben Handlungsbedarf bei der Konzeption der Sicherheitsmassnahmen in Abhängigkeit vom Schutzbedarf der Informationen und bei den damit verbundenen Risiken, oft auch schon im Bereich des sog. Grundschutzes, welcher mit Standard-Sicherheitsmassnahmen ein Mindestschutzniveau sicherzustellen versucht.

Sowohl bei Vorabkontrollen als auch bei Kontrollen begegnet die ASD immer wieder der Aussage, dass Software-Produkte oder Cloudlösungen bereits von vielen Firmen eingesetzt würden. Die Unterschiede der rechtlichen Anforderungen an öffentliche Organe im Vergleich zu jenen an Unternehmen sind oft nicht bekannt.

Im Gegensatz zu einem Unternehmen hat jedes öffentliche Organ von Gesetzes wegen eine öffentliche Aufgabe zu erfüllen. Diese wird in den Grundsätzen jeweils in einem Gesetz (mehr oder weniger) konkret umschrieben. Damit das öffentliche Organ die Aufgabe erfüllen kann, ist es regelmässig darauf angewiesen, auch Personendaten bearbeiten zu können, was es unter Einhaltung verschiedenster Vorgaben des IDG auch darf. Dies ist etwa dann der Fall, wenn es die Personendaten zur Erfüllung der gesetzlichen Aufgaben tatsächlich benötigt. Wenn es die Bearbeitung von Personendaten einem Dritten überträgt, muss es sicherstellen, dass diese vom beauftragten Dritten nur so bearbeitet werden, wie es das öffentliche Organ selbst tun dürfte. Im Gegensatz dazu hat ein Unternehmen zwar ebenfalls Vorgaben aufgrund der bundesrechtlichen Datenschutzgesetzgebung (DSG) zu beachten. Diese unterscheiden sich in vielen Punkten jedoch von denjenigen, welche das kantonale IDG für ein öffentliches Organ vorsieht. Insbesondere bestehen im DSG unterschiedliche Rechtfertigungsgründe für die Bearbeitung von Personendaten, welche das kantonale IDG nicht kennt. So kann ein Unternehmen beispielsweise Personendaten mittels Einwilligung durch die betroffene Person erheben und bearbeiten. Die Einwilligung ersetzt dann die für ein öffentliches Organ zwingend notwendige gesetzliche Grundlage. Folglich kann es im konkreten Fall vorkommen, dass ein Software-Produkt oder eine Cloudlösung von einem Unternehmen eingesetzt werden darf, von einem öffentlichen Organ hingegen nicht oder gegebenenfalls nur unter Einhaltung unterschiedlichster (rechtlicher, organisatorischer und technischer) Massnahmen.

Auch in diesem Berichtsjahr konnten wieder bei mehreren Vorabkontrollen Synergien mit den Datenschutzbeauftragten anderer Kantone genutzt werden. Dabei ging es um den Einsatz von Produkten bzw. Lösungen, die schon in anderen Kantonen in Betrieb sind oder deren Einsatz geplant ist und die die entsprechenden Datenschutzbehörden mit ähnlichem Fokus bereits geprüft hatten.

4

KONTROLLTÄTIGKEIT

Im Rahmen von datenschutzrechtlichen Kontrollen prüft die ASD die Umsetzung der rechtlichen, organisatorischen und technischen Vorgaben. Grundlage dafür bilden die eingereichten Unterlagen, Interviews mit den Verantwortlichen sowie die vor Ort vorgefundenen Massnahmen und Stichproben. Anders als bei der präventiven Vorabkontrolle während der Konzeption wird hier die Einhaltung der Vorgaben im laufenden Betrieb geprüft.

Die Aufsichtsstelle Datenschutz pflegt eine rollende, risikobasierte Kontrollplanung. Dies führt dazu, dass die Planung der Kontrolle und ihre Durchführung nicht zwingend im selben Jahr stattfinden. Ebenfalls zur Kontrolltätigkeit zählt die Rapportierung der Umsetzung von Empfehlungen aus in Vorjahren erfolgten Kontrollen. Die ASD geht davon aus, dass ihre Empfehlungen der Dringlichkeit entsprechend in angemessener Frist umgesetzt werden. In der Regel sollten die Massnahmen spätestens innert zwölf Monaten umgesetzt werden können.

Kontrollen bewirken nebst den konkreten Erkenntnissen zum Handlungsbedarf immer auch eine Sensibilisierung hinsichtlich effektiven Datenschutzes und der Angemessenheit der Informationssicherheitsmassnahmen.

4.1 KINDES- UND ERWACHSENENSCHUTZBEHÖRDEN

Die Tätigkeiten der Kindes- und Erwachsenenschutzbehörden (KESB) vereinen verschiedene Risiken für die Betroffenen: Bei den KESB werden besondere Personendaten bearbeitet, was grundsätzlich das Risiko einer Datenschutzverletzung erhöht. Weitere Risiken ergeben sich durch die interdisziplinäre Zusammenarbeit, die Vielzahl an Schnittstellen mit zahlreichen anderen öffentlichen Organen sowie privaten Mandatsträgern und durch die damit verbundene häufige Bekanntgabe von Personendaten. Hinzu kommt, dass die Datenbearbeitung oft durch Outsourcing-Partner erfolgt und eine grössere Anzahl von Personen von der Datenbearbeitung betroffen ist.

Die Datenschutzkontrolle umfasste im Berichtsjahr u. a. folgende Bereiche: Einhaltung der datenschutzrechtlichen Vorgaben in den Standardprozessen bei Kindesschutzmassnahmen und fürsorgerischer Unterbringung, Datenschutzorganisation, Risikomanagement, Informationssicherheits- und Datenschutzkonzepte sowie Archivierungs- und Löschkonzepte. Eine weitergehende technische Prüfung der Systeme war nicht Gegenstand der Prüfung.

Das Bewusstsein für die Bedeutung der Einhaltung der datenschutzrechtlichen Bestimmungen ist in hohem Masse vorhanden. Es liegen keine Hinweise darauf vor, dass datenschutzrechtliche Vorschriften vorsätzlich verletzt wurden oder Personendaten zu anderen als den gesetzlich vorgesehenen Zwecken verwendet wurden.

Die ASD hat in verschiedenen Bereichen einen Handlungsbedarf festgestellt, namentlich bei der Formalisierung von Informationsflüssen sowie der Instruktion von und Aufsicht über die Beistände, insbesondere der externen. Zu bemängeln war zudem der zu umfassende Zugriff auf Informationen durch zu viele Personen innerhalb der kontrollierten KESB.

Im Bereich der Informationssicherheit haben wir beispielsweise festgestellt, dass die Analyse und Konzeption von Sicherheitsmassnahmen nicht vollständig vorhanden sind. Zudem ist die Sicherstellung der Integrität und Nachvollziehbarkeit von Bearbeitungen besonderer Personendaten nicht ausreichend gewährleistet. Gewisse Mängel im Bereich der Informationssicherheit sind aus Sicht der ASD auch darauf zurückzuführen, dass der KESB kein Sicherheitsbeauftragter bzw. keine Sicherheitsbeauftragte zur Verfügung steht.

Auch stellte die ASD Lücken in den Vertragswerken mit IT-Unternehmen fest, die im Auftrag der KESB Personendaten bearbeiten. Die entsprechenden Verträge regeln die Rahmenbedingungen für die rechtmässige Datenbearbeitung nicht ausreichend. Die ASD hielt bei ihren Empfehlungen fest, dass die Anforderungen bei Neuausschreibungen von Service-Dienstleistungen hinsichtlich Datenschutz und Informationssicherheit ausreichend klar zu formulieren seien und ein entsprechendes Projekt der ASD vor der Ausschreibung, spätestens aber in der Konzeptphase, zur Vorabkontrolle vorgelegt werden müsse.

Die in dieser Datenschutzkontrolle gemachten Feststellungen und die darauf basierenden Empfehlungen betreffen die kontrollierte KESB. Nichtsdestotrotz geht die Aufsichtsstelle Datenschutz davon aus, dass einige der Empfehlungen auch bei anderen KESB eine Verbesserung des Daten-

schutzes und der Informationssicherheit bewirken würden. Aus diesem Grund regte die Aufsichtsstelle Datenschutz an, bei der Umsetzung der Empfehlungen wo möglich und sinnvoll gesamtkantonale Ansätze zu verfolgen.

4.2 SOZIALHILFEBEHÖRDE

Bei der Sozialhilfebehörde werden wie bei der Kindes- und Erwachsenenschutzbehörde besondere Personendaten bearbeitet. Weitere Risiken beinhaltet die Vielzahl an Schnittstellen und die damit verbundene häufige Bekanntgabe von Personendaten infolge interdisziplinärer Zusammenarbeit mit anderen öffentlichen Organen sowie Personen. Zudem besteht eine gesetzliche Grundlage für die verdeckte Bearbeitung von Personendaten. Die Datenbearbeitung durch Outsourcing-Partner ist erfahrungsgemäss mit zusätzlichen Risiken verbunden. Ferner ist eine nicht unerhebliche Zahl von Personen von der Datenbearbeitung betroffen. Deshalb wurde die Sozialhilfe einer grösseren Gemeinde für die Kontrolle ausgewählt.

Die Datenschutzkontrolle beinhaltete u. a. die Erhebung von Personendaten bei einem Unterstützungsgesuch, die Instruktion von sowie Aufsicht über externe Dienstleister, sowohl im Bereich der fallunterstützenden Sachverhaltsabklärung betreffend Bedürftigkeit als auch im IT-Bereich. Ebenfalls waren die Transparenz der Datenbearbeitung sowie die getroffenen organisatorischen und technischen Massnahmen zur Wahrung des Datenschutzes und der Informationssicherheit Gegenstand der Prüfung. Ausserdem wurde die Umsetzung weiterer datenschutzrechtlicher Vorgaben, wie z. B. zur Datenbearbeitung im Auftrag, zur Verhältnismässigkeit, zur Gewährung der datenschutzrechtlichen Rechte der betroffenen Personen und zur Aufbewahrung und Löschung von Daten, kontrolliert.
Das Bewusstsein für die Bedeutung der Einhaltung der datenschutzrechtlichen Bestimmungen ist bei der kontrollierten Stelle in hohem Masse vorhanden. Es liegen keine Hinweise vor, dass datenschutzrechtliche Vorschriften vorsätzlich verletzt wurden oder Personendaten zu anderen als den gesetzlich vorgesehenen Zwecken verwendet wurden.

Im Rahmen der Kontrolle hat die ASD festgestellt, dass gewisse gesetzliche Anforderungen des Datenschutzes und der Informationssicherheit bei der Datenbearbeitung teilweise nicht angemessen erfüllt werden und entsprechend Handlungsbedarf besteht, um ein angemessenes Niveau hinsichtlich Datenschutz und Informationssicherheit zu erreichen.

Betroffen ist namentlich der Bereich der Informationsbeschaffung bei neuen Unterstützungsgesuchen hinsichtlich der Einhaltung der gesetzlich vorgesehenen Kaskade. Zudem ergab die Kontrolle, dass der interne Informationszugang zu umfassend gewährt wird, was dem «Need-to-know-Prinzip» als Konkretisierung des Verhältnismässigkeitsprinzips nicht genügt.

Handlungsbedarf hat die ASD bei den Vertragswerken mit Unternehmen festgestellt, die im Auftrag der Sozialhilfe Personendaten bearbeiten. In den entsprechenden Verträgen waren die Rahmenbedingungen für die Datenbearbeitung teilweise nicht angemessen geregelt.

Weitere Feststellungen machte die ASD bei der unzureichenden Gewährleistung der Informationssicherheit. Handlungsbedarf stellte sie beispielsweise in folgenden Bereichen fest: Nachvollziehbarkeit der Datenbearbeitungen besonderer Personendaten sowie bei der Analyse der IT-Prozesse unter Berücksichtigung der zu unterstützenden Geschäftsprozesse und der Informationssicherheit. Damit fehlen diesbezügliche verbindliche Verpflichtungen der externen Dienstleister.

4.3 DATENERHEBUNG IM RAHMEN VON E-GOVERNMENT-PLATTFORMEN (ONLINE-SCHALTERN)

Im Rahmen einer Datenschutzkontrolle bei einer Gemeinde im Kanton Basel-Landschaft stellte die Aufsichtsstelle fest, dass bei Online-Dienstleistungen vereinzelt Informationen erhoben werden, die im entsprechenden Prozess nicht erfasst werden dürfen.

Einige Gemeinden des Kantons bearbeiten mittels einer E-Government-Plattform Personendaten ihrer Einwohnerinnen und Einwohner, welche diese durch Eingabe in den entsprechenden Formularen via Online-Schalter o. ä. zur Verfügung stellen. Hierbei muss beachtet werden, dass ausschliesslich Personendaten bearbeitet (hier: erhoben) werden dürfen, wenn dafür eine gesetzliche Grundlage besteht oder dies zur Erfüllung der jeweiligen gesetzlichen

Aufgabe erforderlich ist. Dabei ist stets auch die Verhältnismässigkeit zu berücksichtigen («so wenig wie möglich, so viel wie nötig», vgl. § 9 Abs. 3 IDG). Dies gilt unabhängig davon, dass Gemeinden entsprechende Daten basierend auf gesetzlichen Grundlagen wie Registerharmonisierungsgesetz (RHG, SR 431.02) im Register führen müssen. Das für Online-Formulare Erwähnte gilt selbstverständlich auch für Papierformulare. Bei Online-Formularen bestehen jedoch zusätzliche Risiken des Datenabflusses im Internet.

Nicht korrekt ist, wenn z. B. beim Formular für Auskünfte oder Mieterwechsel die Konfession angegeben werden muss. Die Kenntnis der Konfession ist zur Abwicklung dieser Prozesse weder erforderlich noch besteht dafür eine entsprechende Gesetzesgrundlage.

Für gewisse Leistungen einzelner Gemeinden (wie beispielsweise für Auskünfte, Mieterwechsel) wurden die Kundinnen und Kunden zu Verifizierungszwecken zusätzlich aufgefordert, ihre AHV-Nummer in der Online-Maske einzugeben. Das Bundesgesetz über die Alters- und Hinterlassenenversicherung (AHVG) regelt den Umgang mit der AHV-Versichertennummer. Diese darf ausserhalb der Sozialversicherung des Bundes nur dann systematisch verwendet werden, wenn ein Bundesgesetz dies vorsieht und der Verwendungszweck sowie die Nutzungsberechtigten bestimmt sind oder wenn ein kantonales Gesetz dies vorsieht. Vorliegend war nicht ersichtlich, dass die Gemeinden aufgrund eines kantonalen oder eidgenössischen Gesetzes legitimiert sind, die AHV-Versichertennummern ihrer Einwohner und Einwohnerinnen, z. B. bei Auskünften, zu erheben.

Die Aufsichtsstelle fokussierte sich im Berichtsjahr in einem ersten Schritt auf Gemeinden, die Formulare mit besonderen Personendaten wie Konfession und AHV-Nummer beim selben Web-Provider publizieren. So sollte eine koordinierte und damit kostensparende Anpassung der Formulare ermöglicht werden. Bis zum Ende des Berichtsjahres hatten ausser einer Gemeinde alle angeschriebenen Gemeinden die entsprechenden Anpassungen vornehmen lassen.

4.4 SCHENGEN-KONTROLLE

Mit der Übernahme des Schengen-Acquis verpflichtete sich die Schweiz zu gewährleisten, «dass eine unabhängige Behörde unabhängig die Rechtmässigkeit der Verarbeitung personenbezogener SIS-Daten in ihrem Hoheitsgebiet und deren Übermittlung aus ihrem Hoheitsgebiet (…) überwacht». Die kantonalen Datenschutzbeauftragten sind deshalb gehalten, periodisch die Rechtmässigkeit der Bearbeitung personenbezogener Daten im Schengener Informationssystem (SIS) zu kontrollieren (vgl. Art. 60 Beschluss 2007/533/JI bzw. Art. 44 Verordnung (EG) 1987/2006 sowie Art. 55 N-SIS-Verordnung).

Im Berichtsjahr wurde das kantonale Amt für Migration und Bürgerrecht (AFMB) für diese Schengen-Kontrolle ausgewählt. Im Dezember 2019 führte die ASD dort eine Datenschutz-Prüfung durch. Die Kontrolle fokussierte die Einhaltung der rechtlichen Vorgaben bei der Nutzung des Schengener Informationssystems (SIS) und umfasste insbesondere das Berechtigungskonzept bzgl. SIS-Abfragen, die Rechtmässigkeit der konkreten SIS-Abfragen sowie die Nutzung der SIS-Informationen, z. B. für Papierdossiers und einzelne Schutzmassnahmen. Als Basis für die Beurteilung der Rechtmässigkeit der SIS-Abfragen dienten Stichproben aus entsprechenden Abfrage-Protokollen (Logs) des SIS-Betreibers Bundesamt für Polizei (fedpol).

Der Kontrollbericht wird für das erste Halbjahr des Jahres 2020 erwartet.

5

ÖFFENTLICHKEITSPRINZIP

Die Landeskanzlei hat der Aufsichtsstelle Datenschutz in Nachachtung von § 13 Abs. 6 IDV die folgenden Zahlen der im Berichtsjahr bei den Direktionen eingegangenen Gesuche um Zugang zu Informationen gemäss § 23 IDG gemeldet.

Direktion	Gesuche 2018	Gesuche 2019	gutgeheissen	teilweise gutgeheissen	abgewiesen
BKSD	0	0	0	0	0
BUD	0	3	2	0	1
FKD	1	0	0	0	1
SID	4	4	3	0	1
VGD	5	8	0	4	4
LKA	3	13	5	0	8
Total	**13**	**28**	**10**	**4**	**15**

Die Zunahme der Zugangsgesuche um mehr als 100% gegenüber dem Vorjahr ist primär auf die bei der Landeskanzlei eingegangenen Gesuche zurückzuführen, wobei die Landeskanzlei auch für Gesuche zuständig ist, die den Regierungsrat betreffen. Drei der Gesuche betrafen dasselbe Ereignis. Zudem wurde auf einige der Gesuche mangels Zuständigkeit nicht eingetreten. Es bleibt abzuwarten, ob die Zunahme der Zahlen auf solche einmaligen Ereignisse zurückzuführen ist oder ob dies den Beginn eines Trends zeigt, wie er zum Beispiel auf Bundesebene durchaus festzustellen ist. In der Beratungstätigkeit der ASD konnte keine signifikante Erhöhung der Anfragen in diesem Bereich festgestellt werden. Bei gewissen Beratungsanfragen konnte die ASD eine Zunahme der Komplexität der Fälle feststellen. Dies lässt sich durchaus auch mit Beobachtungen in anderen Kantonen sowie auf Bundesebene vereinbaren.

6

ZUSAMMENARBEIT

6.1 ZENTRALE INFORMATIK (ZI)

Die ASD trifft sich periodisch mit der Leitung der ZI und dem kantonalen Sicherheitsbeauftragten, der aktuell bei der ZI angegliedert ist. Bei diesem wertvollen Informationsaustausch werden konkrete Projekte, methodische Grundlagen und allfällige künftige Herausforderungen thematisiert. Auch ausserhalb dieser institutionalisierten Treffen fand im Berichtsjahr ein konstruktiver Austausch mit der ZI statt.

6.2 FACHGRUPPE INFORMATIONSSICHERHEIT (FIS)

Die ASD nimmt an den Sitzungen der FIS als Gast mit beratender Stimme teil. So kann die ASD bereits zu einem sehr frühen Zeitpunkt Stellung nehmen und Anliegen des Datenschutzes können frühzeitig eingebracht und berücksichtigt werden. Im Berichtsjahr konnte die ASD in dieser Rolle nebst Beratung bei aktuellen Themen auch Unterstützung bieten bei der Konzeption einer Benutzer-Protokollierung beim Einsatz von Systemtools, Verschlüsselungsfragen und der Einstufung des Schutzbedarfs.

6.3 DATENSCHUTZBEHÖRDEN ANDERER KANTONE

Die Zusammenarbeit mit Datenschutzbehörden anderer Kantone ist für die ASD wichtig. Auch wenn jeder Kanton seine eigenen rechtlichen Eigenheiten hat und die jeweilige Datenschutzbehörde unabhängig ist, können Informationen und Sachverhalte sowie mögliche Lösungsansätze gewinnbringend ausgetauscht werden. Das Rad muss nicht jedes Mal neu erfunden werden. Die ASD profitiert vom Wissen und der Einschätzung anderer Datenschutzbehörden. So können beispielsweise bei Vorabkontrollen Informationen zu Technologien oder IT-Lösungen ausgetauscht werden, die auch in anderen Kantonen im Einsatz sind. Dies wirkt sich positiv auf die Qualität und die Effizienz aus.

Oft erfolgt die Zusammenarbeit mit anderen Datenschutzbehörden fallspezifisch. Vor allem bei Lösungen, die von zwei oder mehreren Kantonen gemeinsam genutzt werden, sind die Zusammenarbeit und der Austausch zu rechtlichen, organisatorischen und technischen Aspekten unerlässlich.

privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, fördert die Zusammenarbeit unter den Schweizer Kantonen, Gemeinden und dem Bund auf dem Gebiet des Datenschutzes durch ständigen Informationsaustausch. Sie bietet auch den Rahmen für eine gute Zusammenarbeit der Aufsichtsbehörden und unterstützt so den wirkungsvollen Einsatz der Ressourcen.

Die ASD ist in folgenden, für sie sinnvollen privatim-Arbeitsgruppen vertreten:

6.4 AG-ICT

Die Arbeitsgruppe ICT fördert den Austausch der Informatiker und Informatikerinnen, die bei einer Datenschutzbehörde arbeiten. Der Schwerpunkt im Berichtsjahr lag bei gemeinsamen Stellungnahmen sowie beim Austausch zu geplanten und durchgeführten Datenschutzprüfungen und Vorabkontrollen.

Ausserhalb der periodischen Treffen findet unter den Teilnehmenden ein reger Austausch zu konkreten Projekten sowie kantonsübergreifenden Lösungen und Umsetzungen in den einzelnen Kantonen statt.

6.5 AG-SICHERHEIT

Die Arbeitsgruppe Sicherheit traf sich im Berichtsjahr im Juni sowie im September jeweils zu einer Sitzung. Neben der Besprechung von aktuellen Fällen aus den Kantonen waren insbesondere das Bedrohungsmanagement sowie der interkantonale Informationsaustausch im Polizeibereich Hauptthemen. Intensive Diskussionen fanden im Berichtsjahr auch über den Einsatz von Apps zur Parkraumbewirtschaftung und Bezahlung von Parkgebühren statt. Weiter wurde 2019 die Form der künftigen Arbeit der AG-Sicherheit diskutiert. Es wurde u. a. festgelegt, dass der unterjährige Austausch per Mail über relevante Themen intensiviert werden soll.

6.6 AG-DIGITALE VERWALTUNG

Die Arbeitsgruppe Digitale Verwaltung traf sich im Berichtsjahr dreimal. Behandelt wurden u. a. Themen wie E-Voting, Datenschutzfolgeabschätzung und Vorabkonsultation sowie die Meldung von Datenschutzverletzungen.

Das Merkblatt von privatim zum Cloud-Computing wurde im Berichtsjahr angepasst.

6.7 KOORDINATIONSGRUPPE ZUM SCHENGENER INFORMATIONSSYSTEM (SIS)

Diese Arbeitsgruppe ist ein gesetzlich vorgesehenes Gremium, das die Zusammenarbeit und Koordination zwischen den Datenschutzbeauftragten der Kantone und des Bundes bei Kontrollen im Schengen-Bereich erleichtern soll. Betroffen sind insbesondere die Bearbeitung von Personendaten durch Strafverfolgungsbehörden, der Strafvollzug und der Migrationsbereich. Die Arbeitsgruppe trifft sich zweimal jährlich, um die Entwicklungen im Schengen-Bereich zu verfolgen, über erfolgte Kontrollen zu berichten und die Methodik der Kontrollen abzustimmen.

Ein zentrales Thema im Berichtsjahr war die Besprechung der Evaluation, die Vertreter anderer Schengen-Staaten 2018 turnusgemäss in der Schweiz durchgeführt hatten. Wie stets wurde die Kontrolle beim Bund sowie in einem Kanton durchgeführt. Dieses Mal war der Kanton Luzern an der Reihe. Der im Frühjahr 2019 erstellte Bericht enthielt eine Reihe von Empfehlungen zuhanden der kontrollierten Organe, wobei gewisse Feststellungen nach einer Analyse auch teilweise oder ganz auf andere Kantone übertragbar sind. So hielt der Bericht u. a. fest, dass die kontrollierten Datenschutzbehörden über zu wenig Ressourcen verfügten, um ihre durch die Schengener Abkommen auferlegten Pflichten erfüllen zu können. Defizite wurden ebenfalls festgestellt bei der Häufigkeit der Kontrollen des Visa-Systems sowie des Schengener Informationssystems. Sowohl dem Bund als auch dem kontrollierten Kanton wurde empfohlen, diese Kontrollen häufiger durchzuführen.

7

SCHULUNGEN UND REFERATE

Die Schulungen und Referate der ASD sollen die Teilnehmenden für die Themen Datenschutz und/oder Informationssicherheit sensibilisieren und sie dazu befähigen, Aufgaben und Fragestellungen in diesem Bereich besser und somit auch effizienter zu bewältigen. Sie sind geeignete Werkzeuge für die Stärkung des Datenschutzes und einen möglichst sicheren Umgang mit Daten.

Auch in diesem Berichtsjahr hat die Aufsichtsstelle Datenschutz wieder diverse Schulungen und Referate abgehalten. Die Anzahl blieb mit elf gegenüber dem Vorjahr fast unverändert. Wie immer wurden Schulungen bei den Auszubildenden im Rahmen der überbetrieblichen Kurse durchgeführt. Auch die Polizeiaspiranten und -aspirantinnen sind mittlerweile Stammgäste, ebenso wie das Personalamt im Kurs zur Einführung in das Datenschutzrecht. Die Veranstaltung des Personalamtes zum Öffentlichkeitsprinzip konnte hingegen aufgrund mangelnder Nachfrage nicht durchgeführt werden. Bei diesen Kursen handelt es sich um eher allgemeine Referate, die den öffentlichen Organen einen Überblick über das IDG und die Grundprinzipien des Datenschutzes geben sollen. Diese allgemeinen Schulungen leisten aus Sicht der Aufsichtsstelle einen bedeutenden präventiven Beitrag zum Schutz der Personendaten, da sie die grundsätzlichen Fragestellungen des Datenschutzrechts darstellen, wie sie bei jedem öffentlichen Organ in der einen oder anderen Form anzutreffen sind.

Daneben gibt es aber immer auch Bedarf für themenspezifische Referate und Schulungen, die für einen kleineren Kreis von Personen wichtig sind und somit etwas mehr in die Tiefe gehen können. So war die Aufsichtsstelle Datenschutz beispielsweise von den Schulsozialarbeitern und -arbeiterinnen eingeladen worden, die bezüglich Informationsfluss sehr anspruchsvolle Situation in deren Zuständigkeitsbereich datenschutzrechtlich auszuleuchten. Ebenfalls eingeladen wurde die Aufsichtsstelle zum jährlichen Gesamtanlass der Staatsanwaltschaft Basel-Landschaft. Neben der Vorstellung ihrer Tätigkeit im Allgemeinen waren insbesondere die anstehenden Änderungen des Informations- und Datenschutzgesetzes und die Auswirkungen auf die Staatsanwaltschaft Thema des Referates.

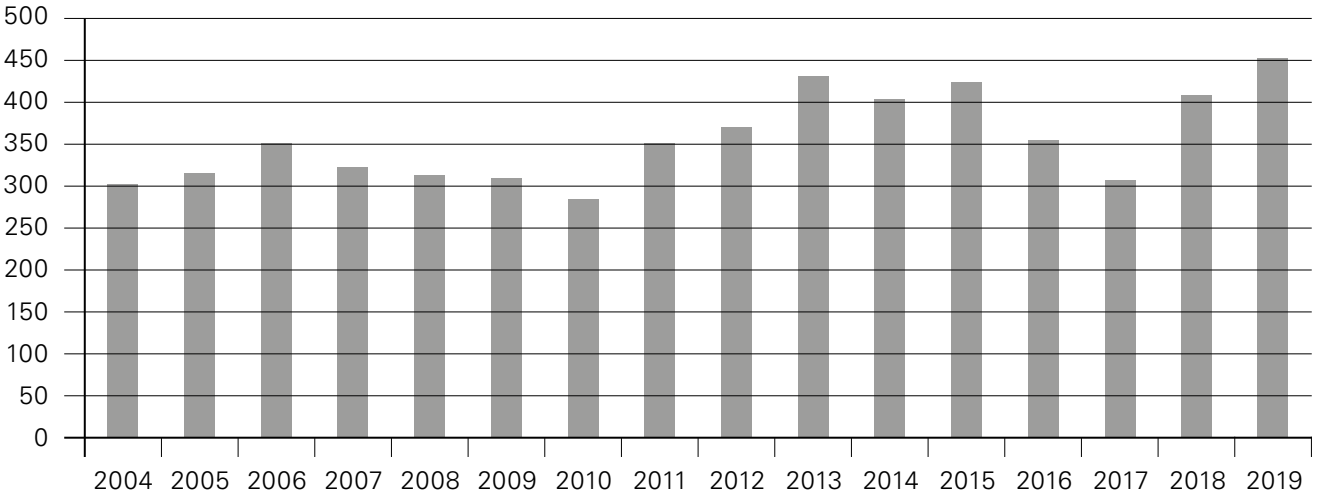
Auch im Bereich der Vorabkontrolle hatte die Aufsichtsstelle mehrmals Gelegenheit, die rechtlichen, organisatorischen und technischen Rahmenbedingungen sowie die etablierte Praxis einem interessierten Publikum näher zu bringen, zum einen bei einem Referat und Erfahrungsaustausch mit Informationseignern, zum anderen an einem Anlass für «Rechtschaffende».

Die Aufsichtsstelle ist sich des Wertes von Schulungen und Referaten für die Steigerung des Bewusstseins für den Datenschutz bewusst und ist immer offen für Vorschläge und Themen.

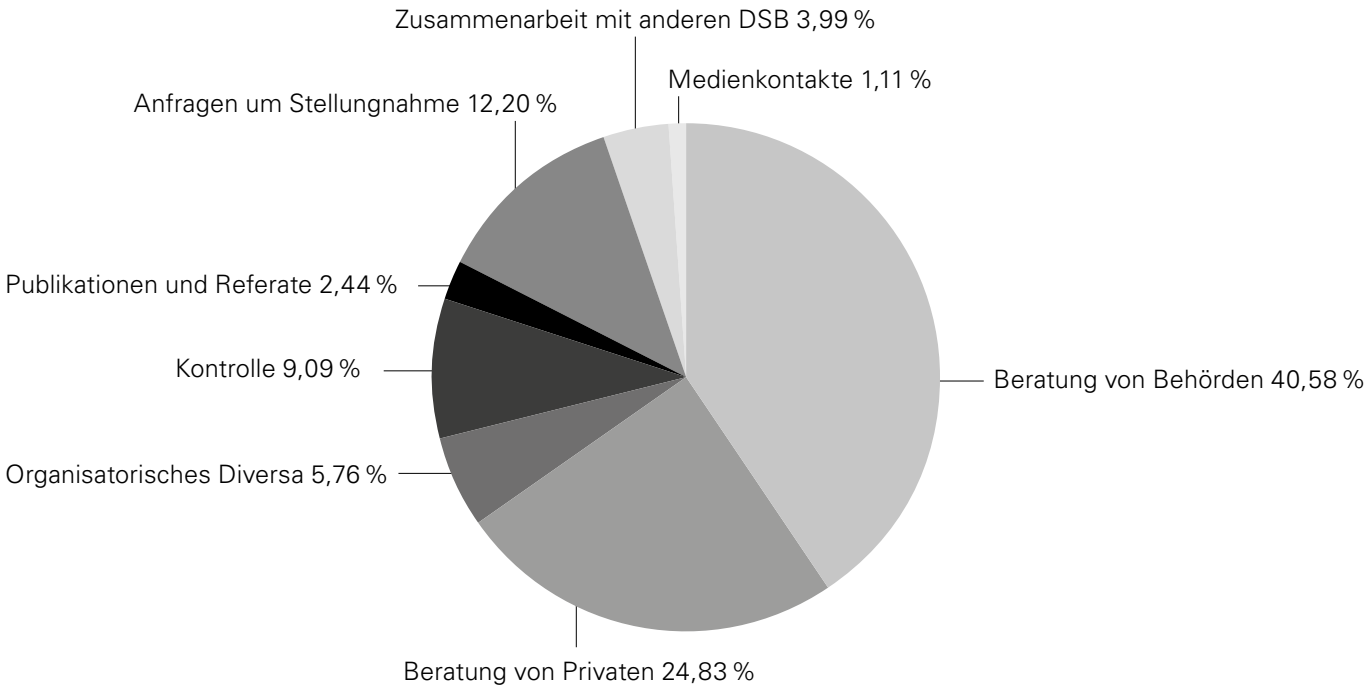
8

ANHANG

GESCHÄFTE



ART DER GESCHÄFTE



(Basis: Anzahl Geschäfte)