BASEL LANDSCHAFT

TÄTIGKEITSBERICHT 2020
DER AUFSICHTSSTELLE DATENSCHUTZ

AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragter
Markus Brönnimann

Stv. Datenschutzbeauftragte
Priscilla Dipner-Gerber
Thomas Held

Akademische Mitarbeitende
Ditmar Freitag
Claudine Müller

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.

ISSN 2673-6462

INHALTSVERZEICHNIS

1

DAS JAHR 2020

1.1 DIE AUFSICHTSSTELLE DATENSCHUTZ (ASD)

Die ASD ist eine unabhängige Aufsichtsbehörde. Sie verfügt über fundiertes Fachwissen bezüglich Datenschutz, dem Umgang mit Informationen, Governance 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 kantonalen öffentlichen Organen[1] Beratungen, Vorabkontrollen, Kontrollen und Schulungen durchgeführt und zu datenschutzrelevanten Erlassen Stellung genommen. Ebenfalls beriet und unterstützte 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 410 Dossiers eröffnet. Der Aufsichtsstelle wurden 31 neue Vorhaben zur Vorabkontrolle vorgelegt. Bei acht Vorhaben entschied die ASD, keine Vorabkontrolle durchzuführen. Bei einem Vorhaben wurde keine Vorabkontrolle durchgeführt, da diese zu spät im Projektablauf vorgelegt wurde und die Empfehlungen im Projekt keine Wirkung mehr hätten entfalten können. Es wurden zwei Datenschutzkontrollen abgeschlossen, 199 Beratungen bei öffentlichen Organen und 78 bei Privatpersonen durchgeführt sowie sechs Schulungen und Referate gehalten. Die ASD wurde für 50 Stellungnahmen angefragt und verfasste weitere 32 Stellungnahmen im Rahmen von Vorabkontrollen. Bei 57 Geschäftsfällen hat die ASD mit Aufsichtsbehörden anderer Kantone zusammengearbeitet.

Der ASD standen für diese Aufgaben 450 Stellenprozente zur Verfügung, welche sich auf sechs Personen verteilten. Ausserdem unterstützten Herr Samuel Metzler und Frau Evi Karapetsa die ASD tatkräftig im Rahmen des jeweils sechsmonatigen Volontariates für Juristen und Juristinnen, welches die ASD auch im Berichtsjahr anbot.

Im Berichtsjahr musste die ASD Tobias Schnelli, Stv. Datenschutzbeauftragter, nach elf Jahren verabschieden. An dieser Stelle danken wir ihm sehr für seinen wertvollen, engagierten Einsatz für den Datenschutz in unserem Kanton.

1.2 COVID-19

Auch für die ASD war das Berichtsjahr gekennzeichnet durch die Corona-Krise. Der Takt des Virus bestimmte über weite Strecken den geschäftlichen Alltag. Etablierte und eingespielte Abläufe, Gewohnheiten und Arbeitsweisen mussten angepasst werden. Arbeiten und Unterricht fanden oft zu Hause statt, physische Treffen nur sehr eingeschränkt und mit Schutzmassnahmen. Ohne digitale Hilfsmittel wäre dies in dieser Form nicht möglich gewesen. Lösungen wurden in grosser Eile gesucht, gefunden und eingesetzt. Um der Lage Herr zu werden, die Ausbreitung des Virus einzudämmen und die Massnahmen für die Bevölkerung und die Wirtschaft so wenig einschneidend wie möglich zu gestalten, wurde und wird eine Vielzahl von Daten gesammelt, analysiert und ausgewertet. Bewegungsmuster werden mit (anonymisierten) Mobiltelefondaten erstellt. Wer wo mit wem und wann zusammen war, soll zur Unterbrechung der Ansteckungsketten gespeichert und festgehalten werden. Alter, Anamnesen und Prädispositionen sollen so effizient und schnell wie möglich (online) erfasst und ausgewertet werden können. Ob jemand geimpft ist, bereits eine Covid-19-Erkrankung durchgemacht hat oder zumindest einen negativen Test vorweisen kann, könnte in Zukunft darüber entscheiden, ob er oder sie ein Flugzeug, eine Bar, einen Zug oder andere öffentliche Orte betreten darf.

Einige unserer Grundrechte wurden und werden während der Pandemie eingeschränkt: die Bewegungs-, Wirtschafts- und Versammlungsfreiheit, aber auch teilweise das Grundrecht auf informationelle Selbstbestimmung, der Schutz der Privatsphäre. Diese Grundrechte müssen wo notwendig in einem gewissen Mass zugunsten eines weiteren Grundrechts, wie etwa demjenigen auf Leben und körperliche Unversehrtheit, eingeschränkt werden. Die Aufgabe der Datenschutzbehörden liegt darin, zu prüfen, ob und wie die jeweiligen Eingriffe in die persönlichen Rechte zu rechtfertigen sind.

Auch wenn die jeweilige Lage berücksichtigt werden muss und die Unversehrtheit und das Leben zweifelsohne geschützt werden müssen, bleibt es in ausserordentlichen Situationen wichtig, dass die Privatsphäre respektiert wird. Zur Bekämpfung der Pandemie dürfen ausschliesslich Informationen über uns bearbeitet werden, die dazu wirklich benötigt werden. Diese müssen ausreichend geschützt wer-

1 Zu den öffentlichen Organen zählen die Kantonsverwaltung, die Gemeinden, öffentliche Institutionen sowie Private, die eine öffentliche Aufgabe übernehmen.

den. Die Intensität des Eingriffs in die Persönlichkeitsrechte im Rahmen der Pandemiebekämpfung muss laufend neu beurteilt werden. Dabei muss der Umfang der bearbeiteten personenbezogenen Informationen und der Risiken, die mit dem jeweiligen Einsatz von IT-Lösungen einhergehen, kontinuierlich evaluiert werden. Das Bearbeiten der Daten über die Personen muss – den allgemeinen verfassungsrechtlichen Grundsätzen folgend – immer geeignet, erforderlich und verhältnismässig sein. Hinzu kommt, dass auch in dieser besonderen Situation die Daten vernichtet werden müssen, wenn sie nicht mehr benötigt werden. Wenn anonymisierte Daten den Zweck ebenfalls erfüllen, müssen die Informationen in anonymisierter Form bearbeitet werden. Datenvermeidung und Datensparsamkeit sind nicht bloss Schlagworte, sondern es handelt sich dabei um gesetzliche Vorgaben für die öffentlichen Organe.

Auch die Datenbearbeitung fällt unter die Massnahmen, die das Epidemiengesetz (EpG, SR 818.101) vorsieht: Art. 30 Abs. 2 EpG gibt hier ebenfalls vor, dass die jeweilige Massnahme erforderlich und zumutbar sein muss. Selbst das Bundesgericht stellt in seinem Urteil BGer 1C_273/2020 im Kontext mit Wasserzählern in privaten Haushalten fest: *«Die Datensicherheit allein vermag den Umstand, dass vorliegend mehr Personendaten bearbeitet werden als notwendig, nicht aufzuwiegen. […] Der Grundsatz der Erforderlichkeit bzw. Datenvermeidung und Datensparsamkeit bezweckt jedoch, dass nicht notwendige Daten gar nicht erst erhoben und bearbeitet werden. In diesem Sinne ist auch ihr Schutz besser gewährleistet: nicht existente Daten können nicht missbraucht werden».* Wenn dies beim Wasserverbrauch zu berücksichtigen ist, gilt es für sensitivere Informationen erst recht!

Digitale Lösungen, die ein Arbeiten auch aus dem Homeoffice oder im Fernunterricht ermöglichen, und selbstverständlich auch Lösungen, die direkt zur Pandemiebekämpfung benötigt werden, mussten schnell verfügbar sein. Eine ordentliche Evaluation und vertiefte Prüfung waren nicht in jedem Fall möglich. Die Datenschutzbeauftragten bei Bund und Kantonen haben sich während der Pandemie immer wieder koordiniert und die öffentlichen Organe bei der Suche nach datenschutzkonformen Lösungen beraten und unterstützt. Bei der Beurteilung der Risiken wurde insbesondere die besondere Lage berücksichtigt. So konnten vorübergehend auch Lösungen eingesetzt werden, welche nicht vollumfänglich datenschutzkonform waren – dies aber nach einer zumindest summarischen Prüfung und vor allem immer als «Übergangslösung».

Dass der Datenschutz in der Schweiz ein wichtiges Gut ist, unterstreicht auch die Entwicklung der SwissCovid-App. Hierbei wurde auf der einen Seite das Prinzip «Privacy by Default» ernst genommen, indem beispielsweise die Informationen anonymisiert bearbeitet werden – was für den Zweck und die Funktion der App richtig und ausreichend erscheint. Auf der anderen Seite erkannte der Bundesgesetzgeber, dass die sehr allgemeine Ermächtigung zur Ergreifung von Massnahmen gemäss Epidemiengesetz für eine sehr breite und intensive Datenbearbeitung nicht genügte, und schuf selbst für diese datenschutzfreundliche Anwendung eine gesetzliche Grundlage (Art. 60a EpG (Proximity Tracing, SwissCovid-App)). Aus Sicht der ASD erscheint es notwendig, dass eine Nachbereitung der Pandemie auch aus rechtlicher Sicht dahingehend erfolgt, dass klarere gesetzliche Rahmenbedingungen für solche Fälle geschaffen werden.

Es bleibt zu hoffen, dass der Datenschutz und die Informationssicherheit bei Digitalisierungsvorhaben auch in Krisenzeiten, aber vor allem wieder im Regelbetrieb den notwendigen und berechtigten Stellenwert erhalten. Die Datenschutzbeauftragten werden ihr Möglichstes dazu beitragen.

1.3 CLOUD – HIMMEL ODER HÖLLE? DEFINITIV KEINES VON BEIDEN.

Es gibt Anwendungsfälle, in denen Cloud-Dienstleistungen sinnvoll und passend sind. Aktuell muss aber festgestellt werden, dass der Druck der Anbieterinnen auf Kunden, Services aus einer Cloud zu beziehen, kontinuierlich steigt. Grosse Anbieter stellen in Aussicht, dass sie ihre Produkte künftig ausschliesslich aus der Cloud anbieten möchten – unabhängig davon, ob die Kundin das will und ihre Bedürfnisse, beispielsweise an Sicherheit oder Datensouveränität, durch die jeweiligen Angebote abgedeckt werden oder nicht. Der Markt ist voll von verlockenden Angeboten, die als flexibler und kostensparender angepriesen werden als Lösungen, die selbst («on premise») oder von einem «klassischen IT-Dienstleister» betrieben werden. Der Cloud-Anbieter wirbt dabei mehr oder weniger explizit auch damit, dass er sowohl die Sicherheit als auch die Erfüllung der Fachanforderungen und zusätzlich den Support besser im Griff habe, als dies

eine interne IT je könnte. Die häufig latente Unzufriedenheit vieler Organisationen und Mitarbeitenden mit «ihrer» internen IT-Leistungserbringerin in Kombination mit einem anhaltenden Fachkräftemangel und einer immer schwieriger beherrschbaren Komplexität in der IT erhöhen den Druck zusätzlich. In diesem Umfeld besteht die Gefahr, dass bei der Evaluation, ob eine Lösung «on premise», bei einem «klassischen Outsourcing-Rechenzentrum» oder in einer Cloud betrieben werden soll, nicht alle Aspekte gebührend berücksichtigt und mit der nötigen Objektivität beurteilt und gegeneinander abgewogen werden.

CLOUD-SERVICES
WAS IST ÜBERHAUPT EINE CLOUD-LÖSUNG?

Unbestritten ist, dass es sich bei der Auslagerung in eine Cloud um eine spezielle Form des Outsourcings handelt. In den Datenschutzgesetzen ist bei solchen Vorhaben von einem «Bearbeiten im Auftrag» die Rede. In der Folge beleuchten wir eine Auswahl von cloud-spezifischen Herausforderungen.

Die Grenzen zwischen einem «klassischen Outsourcing» in das Rechenzentrum eines IT-Dienstleisters und Cloud-Dienstleistungen sind zum Teil fliessend. Cloud-Services werden üblicherweise eingeteilt in folgende Dienstleistungsmodelle: «Software as a Service (SaaS)», «Platform as a Service (PaaS)» und «Infrastructure as a Service (IaaS)». Ausserdem können die Betriebsmodelle Private Cloud, Community Cloud, Public Cloud und Hybrid Cloud unterschieden werden[2] . Hierbei wird neben der Frage, was eine Cloud ist, offensichtlich, dass beispielsweise eine Private Cloud (lokal beim Kunden oder exklusive und «gesicherte» Instanz für einen Kunden) nicht mit einer Public Cloud verglichen werden kann. Auch unterscheiden sich bei den Dienstleistungsmodellen die Einflussmöglichkeit und Abhängigkeit der Auftraggeberin zwischen einer IaaS- und einer SaaS-Lösung stark.

ORTSUNGEBUNDENHEIT UND SUBUNTERNEHMEN

Eine zentrale Technologie bei Cloud-Services ist die Virtualisierung, die eine Entkopplung der Software von der «Umgebung» ermöglicht, sodass die Anbieterin ihre Services schnell und relativ einfach duplizieren oder verschieben kann – in ein beliebiges Rechenzentrum auf der Welt. Oft besteht ein Service für den Kunden aus mehreren (Cloud-)Services, die die Anbieterin selbst betreibt oder wiederum bei einem anderen Cloud-Anbieter einkauft. Dies hat zur Folge, dass Anbieter oft bei ihren jeweiligen Cloud-Angeboten nicht abschliessend ausweisen oder zusichern können, welche Daten wo gespeichert sind, verarbeitet werden oder aus welchen Ländern darauf zugegriffen werden kann oder «muss». Kurzum: Die Datenbearbeitung findet oft irgendwo auf der Welt statt und das Cloud-Angebot wird in vielen Fällen mit dem Einbezug diverser Subunternehmen erbracht. Das öffentliche Organ bleibt dabei in jedem Fall abschliessend für die Einhaltung des Datenschutzes und der Informationssicherheit in der gesamten Lieferkette verantwortlich – auch für die eingebundenen Subunternehmen.

In der Regel gelten jeweils die gesetzlichen Grundlagen vor Ort. Die Bestimmungen können so weit gehen, dass schon nur aus diesem Grund die Nutzung eines Cloud-Service erschwert oder gar verunmöglicht wird. Je nach Bearbeitungsort ist die Bearbeitung ausschliesslich mit der Umsetzung von zusätzlichen Massnahmen zum Schutz der Informationen möglich. Oft geht dies dennoch mit einer Erhöhung des Risikos für das öffentliche Organ einher, welches den Cloud-Service nutzen möchte. Das verbleibende Restrisiko kann aufgrund fehlender oder unzureichender Massnahmen seitens des Cloud-Anbieters zu hoch bleiben und dadurch die Nutzung verunmöglichen. Zusätzlich kommen gesetzliche Grundlagen hinzu, die unabhängig vom Speicher- oder Verarbeitungsort berücksichtigt werden müssen. So verpflichtet beispielsweise der CLOUD Act amerikanische Firmen zur Herausgabe der Daten unabhängig vom Speicherort.

STANDARD-SERVICES

Wenn in der Praxis von der geschäftlichen Nutzung einer Cloud gesprochen wird, kann davon ausgegangen werden, dass in vielen Fällen sogenannte «IT-Commodity-Services» im Fokus stehen. Zugrunde liegt die Annahme, dass ein Service bezogen werden kann, den viele andere Kundinnen in der identischen Form und mit denselben Anforderungen ebenfalls nutzen. Das ist vergleichbar mit dem Strom, der aus der Steckdose kommt und der in der Qualität für den Kunden immer identisch ist, sich beispielsweise nur in der Produktionsart unterscheidet. Bei Cloud-Services entstehen hierbei Skaleneffekte, die sich sowohl auf den Preis als auch auf die Service-Qualität positiv auswirken sollen. Eine zentrale Voraussetzung zur Erreichung dieser Ziele ist, dass alle Kundinnen absolut identische Anforderungen bezüglich Funktion und Sicherheit haben. Hierunter gehören auch

2 Definition nach NIST, National Institute of Standards and Technology des U.S. Department of Commerce

«Standardverträge», denn das Verhandeln und Einhalten von kundenspezifischen Verträgen generiert beim Anbieter zusätzlichen Aufwand und Risiken. Jegliche Abweichungen wirken den Skaleneffekten entgegen und sind somit kaum im Interesse des Anbieters. Im Widerspruch dazu muss aber das öffentliche Organ seinen rechtlichen Pflichten nachkommen.

VERSCHLÜSSELUNG

Neben diversen technischen und organisatorischen Massnahmen sowie vertraglichen Zusatzvereinbarungen[3] gilt für besonders schützenswerte Informationen die Verschlüsselung als zentrale Massnahme der Informationssicherheit. Es gibt in der Zwischenzeit praktisch keinen seriösen Anbieter mehr, der nicht eine Verschlüsselung der Daten verspricht.

Eine zuverlässige Verschlüsselung würde tatsächlich diverse Probleme lösen und das Risiko bezüglich des Schutzziels «Vertraulichkeit» massiv senken. Davon ausgehend, dass eine Verschlüsselung nicht «gebrochen» werden kann und ausschliesslich die Kundin über das Schlüsselmaterial verfügt, würden gar der Speicherort oder der Geschäftssitz der Firma (vgl. CLOUD Act) in den Hintergrund rücken. Die Realität sieht heute aber leider immer noch anders aus.

Es gibt Anbieter, welche die Informationen ausschliesslich beim Transport vom Endgerät des Kunden bis zum Server der Anbieterin verschlüsseln. Das heisst, dass die Daten nach der Übertragung im «Klartext» verarbeitet, intern weitertransportiert und gespeichert werden.

Andere Anbieter verschlüsseln die Daten zusätzlich zur Transportverschlüsselung beim Speichern («at rest»). Das bedeutet, dass, sobald das System beim Cloud-Anbieter gestartet ist und grundsätzlich auf den Speicher zugegriffen werden kann, die Daten für alle im «Klartext» verfügbar sind. Ab diesem Punkt erfolgt der Zugriff auf die Daten so, als wären sie nicht verschlüsselt worden. In einem der ASD zur Prüfung vorgelegten Fall erfolgte die Verschlüsselung des Speichers für alle Kundinnen mit demselben Schlüssel. Dieses Problem versuchen einige Anbieter dadurch zu lösen, dass die Kundin den eigenen Schlüssel bringen kann oder der Anbieter verspricht, dass er pro Kundin einen eigenen Schlüssel generiert. Liegt das Schlüsselmaterial beim Anbieter, muss beachtet werden, dass letztlich das Versprechen oder die vertragliche Zusicherung des Anbieters, dass der Zugriff auf die Schlüssel ausschliesslich mit der Zustimmung des Kunden erfolgt, den hauptsächlichen Schutz darstellt. Kompensierend kann der Anbieter den Schlüssel zusätzlich mit spezialisierter Hardware schützen und in einem unveränderbaren Protokoll die Zugriffe für die nachträgliche Nachvollziehbarkeit aufzeichnen. Das ist in etwa, wie wenn Sie den Schlüssel für Ihr Schliessfach zur Aufbewahrung und Sicherheit bei derselben Bank hinterlegen würden, bei der Sie Ihr Schliessfach haben. Die Bank verspricht, dass die Mitarbeitenden sowie externe Subunternehmern, die das Schliessfach warten und reinigen, den Schlüssel ausschliesslich mit Ihrer Zustimmung nutzen, und installiert zusätzlich über dem Schlüsselsafe, in welchem die Schlüssel aller Kunden aufbewahrt werden, eine Kamera.

Eine Verschlüsselung, die tatsächlich den Effekt hat, welchen sich wohl die meisten Verantwortlichen und Nutzer vorstellen, ist die End-to-End-Verschlüsselung. Dank ihrem Einsatz kann nur die Kundin selbst die Informationen entschlüsseln. Der Verschlüsselungsvorgang erfolgt bei der Kundin und auch das Schlüsselmaterial ist ausschliesslich bei ihr vorhanden. In der Folge müsste somit auch ein grosser Teil der Programmlogik hier ausgeführt werden. In einigen Bereichen wird dies heute tatsächlich so angewandt. So wird beispielsweise bei diversen Chat-Tools der Inhalt der Nachrichten auf diese Weise verschlüsselt. Auch die meisten Mail-Programme verfügen heute über eine Funktionalität, die ermöglicht, dass bei einer Kommunikation zwischen Benutzern mit eigenen Schlüsseln Mails sicher und «persönlich» zugestellt werden könnten.

Bei Software-as-a-Service-Lösungen ist eine End-to-End-Verschlüsselung aber mit dem aktuellen Stand der Technik schwierig und teilweise mit Funktionalitätseinbussen verbunden. Auch herkömmliche Datenbanken, Suchalgorithmen für unstrukturierte Informationen oder auch das Teilen von Informationen mit mehreren Benutzern stellen die Anbieter vor Probleme. Auch das Modell, dass die Anwendung ausschliesslich bei der Anbieterin betrieben wird und der Kunde nur noch das «Bild» präsentiert bekommt, ist nach unserem aktuellen Kenntnisstand mit einer End-to-End-Verschlüsselung nicht umsetzbar.

Ist eine zuverlässige Verschlüsselung nicht möglich, bleibt neben den vertraglichen Zusicherungen und dem Vertrauen in die Anbieterin letztlich nur noch eine Reduktion des

3 Beispielsweise, dass zumindest der Gerichtsstand und das anwendbare Recht des Landes festgelegt werden, in welchem der Service genutzt wird

Schutzbedarfs der Daten als wirklich zuverlässige Massnahme, um die verbleibenden Restrisiken markant zu senken. Dies bedeutet, dass sensitive Daten lokal verarbeitet und gespeichert werden müssen.

ANONYMISIERUNG UND PSEUDONYMISIERUNG

Eine Anonymisierung oder Pseudonymisierung der Personendaten bietet weitere Möglichkeiten. In vielen Fällen dürfte eine solche allerdings nicht wirklich möglich oder praxistauglich sein. So kann beispielsweise der Inhalt eines Briefes an einen Kunden nicht einfach anonymisiert oder pseudonymisiert werden.

ZUSÄTZLICHE PERSONENDATEN

Eine weitere Herausforderung bei diversen Cloud-Services stellt der Umgang mit den bei der Nutzung bei der Anbieterin entstehenden zusätzlichen (Personen-)Daten dar. So werden beispielsweise bei Kommunikationslösungen neben den eigentlichen Inhaltsdaten sogenannte Randdaten bearbeitet. Diese geben darüber Auskunft, wer wann mit wem wie lange kommuniziert hat. Dies sind Informationen, wie sie auch im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) definiert sind. Bei Randdaten kann festgestellt werden, dass diese bei «Standard-Lösungen aus dem Internet» in der Regel nicht in dem Umfang geschützt werden, wie es das BÜPF für Anbieter von Fernmeldediensten vorschreibt. Im Gegenteil: Anbieter lassen sich über die AGB teilweise bestätigen, dass die Daten für weitere Zwecke genutzt werden dürfen. Bei vermeintlich kostenlosen Services bezahlt die Nutzerin so die Dienstleistung letztlich mit der Weiterverwendung ihrer (Personen-)Daten durch die Anbieterin. Im Gegensatz zur Nutzung im privatrechtlichen Bereich, in welchem eine Einwilligung für diese Geschäftspraxis ausreichend ist, kommt ein solches Vorgehen für öffentliche Organe nicht in Frage. Für sie gilt, dass sie sicherstellen müssen, dass die Informationen nur so bearbeitet werden, wie sie es selbst auch tun dürften – daran ändert auch ein (Cloud-)Outsourcing nichts. Das heisst, dass jegliche Datenbearbeitung einer gesetzlichen Grundlage bedarf und dass die Daten ausschliesslich zu dem Zweck bearbeitet werden, zu dem diese erhoben wurden. Ausserdem dürfte es kaum im öffentlichen Interesse liegen, dass staatliche Institutionen die von ihnen eingesetzten IT-Dienste mit der Verwertung von Personendaten «bezahlen». Erwähnenswert an dieser Stelle ist, dass Randdaten nicht so harmlos sind, wie die Bezeichnung vermuten lässt. Nach BÜPF sind diese ausreichend, um eine behördliche Überwachung zu ermöglichen. Ausserhalb der Überwachung können Randdaten (ohne Inhaltsinformationen) zu besonderen Personendaten werden, beispielsweise wenn aufgezeichnet wird, wer eine Online-Therapiesitzung in Anspruch nimmt.

Selbstverständlich gibt es legitime Zwecke, für welche die Leistungserbringer Daten erheben und auswerten dürfen. Dies könnte etwa für die Fehlerbehebung notwendig sein. Zu beachten ist in jedem Fall, dass alle Personendaten, auch die Daten, die bei der Nutzung der Dienste anfallen, mit angemessenen Massnahmen geschützt und nach Ablauf der Aufbewahrungsfrist vernichtet oder zuverlässig anonymisiert werden müssen.

VERANTWORTUNG

Die Corona-Krise hat auch beim Thema Cloud-Dienstleistungen ihre Spuren hinterlassen. Notwendige Informatiklösungen konnten in der gebotenen Eile gar nicht lokal aufgebaut und zur Verfügung gestellt werden. Vor allem in den Bereichen Zusammenarbeit, Ermöglichen von Fernunterricht und im Rahmen der Pandemiebekämpfung waren schnelle Lösungen gefragt. Funktionieren eingeführte Lösungen grundsätzlich, können häufig eine gewisse Trägheit und ein Gewöhnungseffekt beobachtet werden. Diese halten oft so lange an, bis ein ernsthafter Zwischenfall eintritt oder bei genauerer Beurteilung frappante Defizite entdeckt werden. Haben sich die Verantwortlichen zuvor nicht proaktiv und ernsthaft mit den Risiken befasst, müssen sie sich in der Folge zu Recht den Vorwurf gefallen lassen, nicht rechtzeitig gehandelt zu haben. Lösungen, die in der Krise notgedrungen ohne sorgfältige und dem Schutzbedarf der Informationen angepasste Abklärungen eingesetzt wurden, müssen im Nachhinein mit der notwendigen Sorgfalt beurteilt, angepasst und gegebenenfalls ersetzt werden.

Abschliessend gilt festzuhalten, dass die aus der Nutzung von Cloud-Lösungen entstehenden Risiken, die bei Weitem nicht nur Datenschutzaspekte betreffen, von der obersten Leitung einer Organisation verantwortet werden müssen. Auch wenn die interne IT-Abteilung hier einen wichtigen und wesentlichen Beitrag zur Beurteilung und zum Lösungsdesign leisten kann und muss, können die IT-Verantwortlichen dieses Risiko unmöglich alleine verantworten. Auch die Vor-

gaben aus den Datenschutzgesetzen sind diesbezüglich klar: Abschliessend verantwortlich ist das öffentliche Organ und nicht die IT.

Datenschutzbeauftragte können Empfehlungen zum Umgang mit Informationen abgeben und auf die zusätzlichen (hohen) Risiken hinweisen. Sie können und müssen dafür sorgen, dass die Risiken zumindest bekannt sind und diese explizit von den Verantwortlichen akzeptiert werden müssen. Falls den Empfehlungen nicht Folge geleistet wird und die Risiken für die Rechte der betroffenen Personen nachweislich sehr gross sind oder die Bearbeitung gar rechtswidrig ist, kann die Bearbeitung vom Datenschutzbeauftragten mit einer anfechtbaren Weisung beanstandet werden. Wie ein Gericht bezüglich der Risiken bei der Bearbeitung von Informationen mit einem sehr hohen Schutzbedarf in einer Cloud urteilen würde, ist zum heutigen Zeitpunkt mangels Gerichtsentscheiden in der Schweiz unklar.

Weitere Informationen sind auch im Merkblatt «Cloud-spezifische Risiken und Massnahmen» von *privatim* zu finden, welches aktuell überarbeitet wird. U. a. wird das Merkblatt um die Thematik zum Umgang mit zusätzlichen Personendaten, wie beispielsweise Randdaten, erweitert.

1.4 INFORMATIONS- UND DATENSCHUTZGESETZ (IDG)

Das neue IDG wurde am 14. Januar 2021 vom Landrat verabschiedet und soll 2021 in Kraft treten.

Wie bereits mehrfach in den vergangenen Tätigkeitsberichten thematisiert, war eine Revision des kantonalen IDG aufgrund der grossen europäischen Datenschutzreform notwendig geworden, zu der sich auch die Schweiz staatsvertraglich verpflichtet hat. Im vergangenen Jahr nahm die Revision Fahrt auf. Über die Landratsvorlage wurde danach zuerst von der Justiz- und Sicherheitskommission und dann vom Landrat selbst beraten. Die ASD hatte wiederholt Gelegenheit, die SID während des Rechtsetzungsprozesses zu beraten.

Im Kanton Basel-Landschaft entspricht ein grosser Teil der notwendig gewordenen Änderungen der bereits bestehenden Praxis. Diese wird damit gesetzlich geregelt und konkretisiert – insbesondere werden der präventive Datenschutz und die Transparenz gestärkt. Neu hinzu kommt die Meldepflicht bei Datenschutzverletzungen. Anlässlich der Revision wurden auch zwei Motionen des Landrats aufgegriffen. Während die Bestimmung betreffend Pilotversuche unbestritten war, sorgte die vorgesehene Möglichkeit der Verrechnung von Beratungsleistungen der ASD für intensivere Diskussionen. Aufgrund der grösstenteils ablehnenden Rückmeldungen in der Vernehmlassung hatte die Regierung darauf verzichtet, eine Bestimmung vorzuschlagen. Der Landrat folgte dabei der Regierung, zog es aber dennoch vor, die Motion nicht als erledigt abzuschreiben. Damit wird sie bei einer zukünftigen Revision wieder aufgenommen.

Neu wird im Gesetz formuliert, dass das öffentliche Organ gegenüber der ASD nachweisen können muss, dass es die Datenschutzbestimmungen einhält. Bereits heute müssen die öffentlichen Organe u. a. sicherstellen, dass sie ausschliesslich Informationen über und zu Personen bearbeiten, sofern sie dafür eine gesetzliche Grundlage haben. Ebenfalls müssen Prozesse definiert sein, die die Gewährleistung der Rechte der betroffenen Personen operativ sicherstellen. Die neue Bestimmung unterstreicht diese Pflichten der öffentlichen Organe.

Gleiches gilt für die nunmehr ausdrücklich im Gesetz festgehaltene Pflicht, Datenschutzverletzungen («Data Breaches») zu melden. Das öffentliche Organ muss (Sicherheits-) Vorfälle bei der Datenbearbeitung der Aufsichtsstelle und gegebenenfalls auch den Betroffenen melden. Dies gilt auch für Vorfälle, die bei einer Auftragnehmerin des öffentlichen Organs auftreten.

Der Kanton Basel-Landschaft kennt bereits seit dem Jahr 2008 die Vorabkontrolle. Die Umbenennung in «Vorabkonsultation» ist dabei eine rein terminologische Anpassung. Das Gesetz sieht neu aber eine vorgeschaltete Datenschutz-Folgenabschätzung (DSFA) vor. Die durch das verantwortliche öffentliche Organ vorgängig vorgenommene Beurteilung der Risiken für die Grundrechte der durch die Bearbeitung betroffenen Personen war bisher bereits integraler Bestandteil der Vorabkontrolle. Auch das geplante Vorhaben, die Rechtsgrundlagen, der Schutzbedarf sowie die Abhilfemassnahmen mussten schon festgehalten werden. Damit werden mit der Datenschutz-Folgenabschätzung also bereits die Grundlagen für die eigentliche Vorabkonsultation erarbeitet. Sie sind in jedem Fall Voraussetzung für eine geordnete und

auch gesetzeskonforme Durchführung eines Projektes. Diverse der Grundlagen, die hierbei erarbeitet werden, sollten im Projekt laufend weiterentwickelt werden und dienen später im laufenden Betrieb der Sicherheit der Anwendung. Zudem dienen diese Dokumente auch dem Nachweis der Einhaltung der Datenschutzbestimmungen.

Mit den Pilotversuchen wird die Möglichkeit geschaffen, unter bestimmten Voraussetzungen und für eine beschränkte Zeit die Bearbeitung besonderer Personendaten zur Erprobung neuer Verfahren zu ermöglichen, gestützt auf eine Verordnung und nicht wie sonst gefordert auf ein Gesetz im formellen Sinn. Die neue Bestimmung lässt somit dort, wo tatsächlich eine entsprechende Notwendigkeit besteht, eine «experimentelle Gesetzgebung» zu. So lassen sich die Auswirkungen einer geplanten Gesetzesregelung zunächst während einer Pilotphase überprüfen und evaluieren. Nach Ablauf des Pilotbetriebs können die Erkenntnisse bei Fortsetzung des Projekts auf Gesetzesebene berücksichtigt werden. Basel-Stadt kennt diese Bestimmung bereits und hat damit gute Erfahrungen gemacht.

Ebenfalls neu ist die spezialgesetzliche Regelung der Datenschutz-Aufsichtsbeschwerde. Auch hier geht die ASD davon aus, dass sie auf bereits bestehende Prozesse zurückgreifen kann, da sie auch schon unter dem aktuellen Recht Hinweisen und Anliegen aus der Bevölkerung nachgegangen ist und diese aufsichtsrechtlich untersucht hat.

Zudem wird in Anlehnung an das Bundesrecht und die Regelung im Kanton Basel-Stadt eine Koordinationsbestimmung zwischen Datenschutz und Öffentlichkeitsprinzip geschaffen, indem bei Zugangsgesuchen nach § 23 IDG im Ausnahmefall bei einem überwiegenden öffentlichen Interesse Personendaten bekanntgegeben werden können, auch wenn sie nicht anonymisierbar sind.

2
AUS DEM BERATUNGSALLTAG

2.1 E-MAIL-KOMMUNIKATION ZWISCHEN EINER BEHÖRDE UND VERSICHERTEN PERSONEN

Eine Behörde musste aufgrund der Corona-Massnahmen ihre Prozesse umgestalten, denn die Anmeldung bei der Arbeitslosenversicherung war vor Ort nicht mehr möglich. Personen meldeten sich in der Folge meist telefonisch an, und die Unterlagen, die den Kunden normalerweise bei der Anmeldung vor Ort ausgehändigt werden, werden seither per E-Mail übermittelt, sofern die versicherte Person eine E-Mailadresse zur Kommunikation angibt. Die Behörde hatte in diesem Kontext verschiedene Fragen rechtlicher und datensicherheitstechnischer Art.

Der Versand von Merkblättern und leeren Formularen an eine versicherte Person, die ihre Mailadresse angegeben hat, ist zulässig, sofern die Mails zumindest transportverschlüsselt übertragen werden. Die Mailadresse der Person und ihr Verhältnis zur Arbeitslosenversicherung zählen nicht zu den besonderen Personendaten, allerdings sind sie trotzdem angemessen zu schützen.

Eine Einwilligung zu einem gegenseitigen Austausch von teilweise streng vertraulichen Informationen bei einem bekanntermassen unsicheren E-Mail-Übermittlungsweg zu verlangen, wäre jedoch nicht statthaft. Anders gestaltet sich die Sachlage, wenn eine Behörde von Kundinnen und Kunden ungefragt Mails mit streng vertraulichem Inhalt erhält, da sie darauf – ausser mit einem Hinweis auf der Webseite bzw. in den Formularen – keinen Einfluss hat.

Angesichts der aktuellen kantonalen Mailinfrastruktur ist ein Versand streng vertraulicher Informationen nur in einem sepa-

raten, angemessen verschlüsselten Anhang zulässig. Aufgrund der derzeit nicht automatisierten Verschlüsselung beim Mailversand solcher Informationen erscheint der Versand auf dem Postweg einfacher und bei korrekter Adressierung sicherer.
Die ASD empfahl der Behörde ausserdem die Eignungsprüfung von Anmeldeformularen für den Versand über den kantonalen eGov-Formularservice. Mit dieser Lösung kann ein sicherer Übertragungsweg gewährleistet werden.

2.2 VERANTWORTUNG BEI DER GEMEINSAMEN NUTZUNG VON KANTONALEN SERVICES

Gemäss § 6 Abs. 1 des Informations- und Datenschutzgesetzes (IDG, SGS 162) trägt dasjenige öffentliche Organ die Verantwortung für den Umgang mit Informationen, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet.

Bei in der kantonalen Verwaltung mehrfach eingesetzten Informatiklösungen ist davon auszugehen, dass die Zentrale Informatik als kantonaler Dienstleister die Verantwortung für die Bereitstellung der Lösung und allfällige Verträge mit externen Dienstleistern übernimmt. Sie kann allerdings nicht die Verantwortung im Sinne von § 6 IDG übernehmen. Wichtig ist jedoch, dass die Zentrale Informatik (ZI) die Behörden, die den Service nutzen möchten, über die Restrisiken informiert, die trotz dem Ergreifen von Sicherheitsmassnahmen weiterhin bestehen.

Eine kantonale Behörde, die einen solchen neuen Service nutzen wollte, sah sich nicht in der Lage, die Verantwortung für die Restrisiken des Service zu übernehmen und gelangte gemeinsam mit der Zentralen Informatik an die ASD zur Klärung der Rollen.

Tatsächlich können einzelne Behörden nicht den gesamten Service mit einer Vielzahl von angeschlossenen Dienststellen verantworten und sämtliche damit verbundenen Restrisiken mittragen, da sie keinen Einfluss darauf nehmen können. Die einzelnen Dienststellen oder Behörden, die den Service für ihre Aufgabenerfüllung nutzen, müssen jedoch die Verantwortung für ihren Aufgabenbereich tragen, allfällige Restrisiken bei dessen Nutzung beurteilen und darauf basierend den Einsatzentscheid fällen können – dies auch deshalb, weil das Schadensausmass von der behördenspezifischen Konfiguration abhängt.

Die ASD empfahl, diese Verantwortlichkeiten auch in der Service-Vereinbarung (SLA) zwischen der jeweiligen Behörde und der ZI festzuhalten. Mit der Unterzeichnung der SLA sind die Übernahme der behördenspezifischen Verantwortung für den Service geregelt, die Einhaltung der organisatorischen Regelungen bei der Nutzung bestätigt und die Restrisiken festgehalten.

2.3 RAHMENBEDINGUNGEN FÜR HOMEOFFICE BEI GEMEINDEN

Als Folge der vom Bund verordneten Corona-Massnahmen bezüglich Homeoffice gelangten einige Gemeinden an die ASD mit der Frage, was es zu beachten gelte.

Als Erstes braucht es eine Absprache mit den Vorgesetzten und die Erfüllung gewisser Voraussetzungen, auch was die Informationssicherheit betrifft.

Papierakten sollten nur falls zwingend notwendig nach Hause mitgenommen und dort – bei Nichtgebrauch – eingeschlossen werden, strengere kommunale/kantonale Regelungen vorbehalten. Bei der Mitnahme von Dokumenten ist es wichtig, dass diese möglichst in einem geschlossenen und nicht einsehbaren Behältnis transportiert und zu Hause für andere nicht einsehbar aufbewahrt werden. Falls Dokumente auf elektronischen Datenträgern mitgenommen werden müssen, so ist darauf zu achten, dass diese verschlüsselt sind. Es sollten insbesondere keine Dokumente mit personenbezogenen Daten mit nach Hause genommen werden, wenn dies zur Aufgabenerfüllung nicht unbedingt notwendig ist.

Beim Arbeiten im Homeoffice sind einige Schutzmassnahmen zur Gewährleistung der Informationssicherheit zu beachten. In Unkenntnis der Details zur technischen Anbindung der verschiedenen Gemeinden an eine Remote-Access-/VPN-Lösung empfahlen wir, minimale technische und organisatorische Rahmenbedingungen einzuhalten, wenn Mitarbeitende der Gemeinde vom Homeoffice aus auf die Fachapplikationen und die Dateiablage der Gemeinde oder das zentrale Personenregister (arbo) zugreifen. Dazu zählen u. a. der sorgfältige Umgang mit Papierakten zu Hause, ein gesicherter Zugang zu Gemeindeanwendungen (sog. VPN mit 2-Faktor-Authentisierung), Zugriffsschutz und Virenschutz auf dem privaten PC, keine fremde Einsichtsmöglichkeit auf den Bildschirm, diskretes Telefonieren, Verzicht auf den Ver-

sand von geschäftlichen Mails an und von einem privaten Mailkonto, keine lokale Speicherung von Daten, u.s.w.

Wir empfahlen, nach Ende der Corona-Krise den Homeoffice-Anwendungsfall im Detail – evtl. koordiniert für alle Gemeinden – zu evaluieren, um eine stabile Lösung etablieren zu können.

2.4 AUFFORDERUNG ZUR AUSSTELLUNG EINER VOLLMACHT

Eine Privatperson wandte sich an die ASD. Sie war vom Sozialdienst zur Einreichung von Unterlagen aufgefordert worden. Der Aufforderung beigelegt war zudem ein Formular zur Erteilung einer Vollmacht, gestützt auf welche der Sozialdienst bei Dritten weitere Auskünfte einholen wollte. Bei mangelnder Mitwirkung wurde ihr eine Kürzung der Sozialleistungen in Aussicht gestellt. Die Person wollte von der ASD wissen, ob diese Kürzung zulässig sei, falls sie die Vollmacht verweigere.

Die ASD nahm daraufhin mit der betreffenden kommunalen Sozialhilfestelle Kontakt auf. Grundsätzlich ist die Abklärung des Sachverhalts rund um den Bezug von Sozialhilfeleistungen gesetzlich vorgesehen und klar geregelt. Die Informationsbeschaffung folgt einer im Sozialhilfegesetz beschriebenen Kaskade, wonach die Informationen primär bei den Personen, welche Unterstützung beantragen, im Sinne einer Selbstdeklaration eingeholt werden. Besteht danach weiterer Informationsbedarf, kann der Sozialdienst auf dem Wege der Amtshilfe bei weiteren öffentlichen Organen Informationen einholen. Erst wenn danach noch weitere Informationen benötigt werden, ist die antragstellende Person verpflichtet, eine Ermächtigung zur Informationsbeschaffung auszustellen. Das Einholen der Vollmacht stellt somit das letzte Mittel zur Erfüllung der Mitwirkungspflicht dar und darf nur in Ausnahmefällen für ganz spezifische Informationen verlangt werden. Daraus folgt ebenfalls, dass eine Vollmacht sich auf eine konkrete Situation beziehen muss. Eine Blanko-Vollmacht zur umfassenden Informationsbeschaffung wie im konkreten Fall fällt somit ausser Betracht. Im Sinne des Transparenzprinzips der Datenbearbeitung muss eine Person erkennen können, welche Angaben über sie bearbeitet werden und bei welchen Stellen Informationen eingeholt werden. Ebenfalls muss die Konsequenz der Nichteinreichung von Unterlagen oder einer Vollmacht in Form einer Reduktion des Sozialhilfeanspruchs klar erkennbar sein. Die ASD teilte dem Sozialdienst mit, dass einerseits der Prozess zur Einholung der Vollmacht sowie auch die Vollmacht selbst angepasst werden müssten. Der Sozialdienst folgte diesen Empfehlungen umgehend.

2.5 BEKANNTGABE DES GEBURTSDATUMS DER MITGLIEDER EINES MUSIKVEREINS DURCH DIE EINWOHNERDIENSTE

Eine Gemeinde gelangte an die ASD, weil sie von einem öffentlichen Musikverein angeschrieben wurde. Der Musikverein verlangte nach den Geburtsdaten sämtlicher Mitglieder, um an deren Geburtstag jeweils ein Ständchen spielen zu können.

Die ASD teilte der Gemeinde mit, dass sich hier die Frage nach einer Listenauskunft stelle. Damit eine Gemeinde nach Merkmalen (wie vorliegend Adressen) geordnete Daten über mehrere Personen an eine 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 vorliegend fest, dass es sich beim «Ständchenspielen» nicht um einen schützenswerten ideellen Zweck handelt, die Voraussetzungen von § 3 Abs. 3 ARG somit nicht erfüllt und eine Bekanntgabe der Geburtsdaten nicht erlaubt ist. Da der Musikverein seine Mitglieder kennt, muss er die Einwilligung für das Vorhaben direkt bei ihnen einholen. Dies kann bei neuen Mitgliedern bereits bei der Anmeldung mittels Formular geregelt werden.

2.6 DÜRFEN DEM GEMEINDERAT MONATLICH LISTEN DER ZU- UND WEGZÜGERINNEN ZUR EINSICHT ZUR VERFÜGUNG GESTELLT WERDEN?

Eine Gemeindeverwaltung gelangte an die ASD mit der Frage, ob dem Gemeinderat monatlich Listen der Zu- und Wegzüger zur Einsicht zur Verfügung gestellt werden dürfen.

Die ASD legte der Gemeindeverwaltung dar, dass für eine solche Bekanntgabe von Personendaten an ein anderes öffentliches Organ gemäss § 18 Abs. 1 IDG entweder a) eine gesetzliche Grundlage bestehen, b) die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein oder c) die betroffene Person der Bekanntgabe im Einzelfall ausdrücklich zugestimmt haben muss.

Eine direkte gesetzliche Grundlage besteht für die Bekanntgabe der Zu- und Wegzügerinnen nicht. Zudem ist auch nicht ersichtlich, inwiefern eine solche Liste für den Gemeinderat zur Erfüllung seiner Aufgaben erforderlich sein soll. Eine Einwilligung der Betroffenen liegt auch nicht vor. Insofern ist keine der Voraussetzungen erfüllt und eine Bekanntgabe an den Gemeinderat nicht erlaubt. Eine Möglichkeit bestünde jedoch darin, Einsicht in eine Liste zu gewähren, die lediglich die Anzahl der zu- und weggezogenen Personen aufführt (allenfalls aufgeschlüsselt nach Alter und/oder Geschlecht). Denkbar sind des Weiteren Informationen, welche relevant für die Planung sein könnten (z. B. Anzahl Kinder). Diese Planungsdaten könnten anonymisiert werden, wodurch keine Personendaten bearbeitet würden.

2.7 WEITERGABE EINES BRIEFES DURCH DIE GESCHÄFTSPRÜFUNGSKOMMISSION AN DEN GEMEINDERAT

Eine Privatperson gelangte mit folgendem Sachverhalt an die ASD: Sie hatte der Geschäftsprüfungskommission (GPK) einer Gemeinde einen eingeschriebenen Brief mit einer Frage und einem persönlichen Anliegen gesendet. Die GPK leitete diesen Brief daraufhin an den Gemeinderat weiter, inklusive Name und Adresse der ursprünglichen Absenderin. Die betroffene Person wollte von der ASD wissen, ob die GPK dies tun durfte.

Die ASD stellte klar, dass es sich bei den Personalien und dem Brief der betroffenen Person an die GPK um Personendaten handelt. Eine gesetzliche Grundlage, die eine Bekanntgabe von Personendaten der GPK an den Gemeinderat vorsehen würde, konnte nicht ausfindig gemacht werden. Als Zweites prüfte die ASD die Erforderlichkeit der Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe. Die GPK hat die Oberaufsicht über alle Gemeindebehörden und Verwaltungszweige und prüft deren Tätigkeit (§ 102 Gemeindegesetz). Sie kann zur Erfüllung dieser Aufgabe Einsicht in die Akten sämtlicher Organe und Verwaltungszweige nehmen. Die Mitglieder der einzelnen Organe und der Verwaltungsstellen sind verpflichtet, der GPK Auskunft zu erteilen. Die ASD kam jedoch zum Schluss, dass sich daraus keine Pflicht (oder auch nur eine Ermächtigung) zur Bekanntgabe von Personendaten durch die GPK ableiten lässt. Dass die GPK dem Gemeinderat gewisse Informationen weitergibt – namentlich die von der betroffenen Person aufgeworfenen Fragen – erscheint notwendig, zumal anderenfalls die aufgeworfenen Fragen gar nicht beantwortet und die gesetzlich vorgesehene Aufgabe nicht korrekt erfüllt werden könnten. Die Bekanntgabe der Personalien respektive die Weiterleitung des vollständigen Briefes erwies sich unter diesem Blickwinkel aber als nicht erforderlich und war aus datenschutzrechtlicher Sicht folglich unzulässig.

2.8 BEKANNTGABE VON DATEN VERSTORBENER PERSONEN AN DIE BÜRGERGEMEINDE

Eine Gemeinde wandte sich an die ASD mit der Frage, ob ihre bisherige Praxis, alle Todesfälle innerhalb der Gemeinde der Bürgergemeinde bekanntzugeben, den datenschutzrechtlichen Vorgaben entspräche.

Es stellte sich die Frage, ob die Personendaten von Verstorbenen auch vom IDG erfasst sind. Grundsätzlich verwendet das IDG den Begriff der «Person» wie das Zivilgesetzbuch. Demnach endet die Persönlichkeit mit dem Tod. Dies würde bedeuten, dass die Bearbeitung von Daten von Verstorbenen nicht mehr die Anforderungen von § 9 IDG zu erfüllen hätte, da es eben keine *Personen*daten mehr sind. Anders als andere Kantone kennt der Kanton Basel-Landschaft für nicht archivierte Daten von verstorbenen Personen keine ausdrückliche gesetzliche Regelung. Für archivierte Daten ist das Archivierungsgesetz massgebend. Bei diversen öffentlichen Organen werden aber auch Daten von verstorbenen Personen aktiv bearbeitet, was z. B. mit Blick auf das Erbschaftsamt unmittelbar einleuchtet. Damit keine Schutzlücke für die Zeit zwischen dem Tod und der (allfälligen) Archivierung der Daten entsteht, geht die ASD davon aus, dass die Regelungen von § 9 ff. IDG auch in diesem Zeitraum sinngemäss Geltung haben müssen. Zusätzlich enthalten Daten von verstorbenen Personen oft auch gleichzeitig Informationen über lebende Personen, z. B. die Angehörigen. Der datenschutzrechtliche Persönlichkeitsschutz hört nicht unmittelbar nach dem Tod auf. Die ASD prüfte demnach die Anfrage der Bürgergemeinde mit Blick auf die bereits mehrfach zitierten Bestimmungen zur Datenbekanntgabe, § 18 f. IDG: Eine direkte gesetzliche Grundlage, welche die Gemeinde zur Bekanntgabe sämtlicher Todesfälle an die Bürgergemeinde verpflichtet oder ermächtigt hätte, war nicht ersichtlich. Es stellte sich jedoch die Frage, ob die Meldung

zur Erfüllung einer öffentlichen Aufgabe erfolgen musste. Die Bürgergemeinde ist zwecks administrativen und finanziellen Überblicks und korrekter Amtsführung gehalten, ihren Datenbestand zu aktualisieren. Dafür muss sie Kenntnis darüber haben, ob Personen, welche der Bürgergemeinde angehören, verstorben sind. Die Kenntnisnahme von Todesfällen von Nicht-Mitgliedern der Bürgergemeinde ist allerdings zur korrekten Aufgabenerfüllung nicht nötig. Die Bekanntgabe von Todesfällen durch die Gemeinde an die Bürgergemeinde ist somit insoweit rechtmässig, als sie lediglich verstorbene Angehörige der Bürgergemeinde umfasst. Eine Bekanntgabe darüber hinaus ist jedoch nicht zur Aufgabenerfüllung notwendig und aus datenschutzrechtlicher Sicht folglich unzulässig.

2.9 DIE DATENSPERRE UND IHRE DURCHBRECHUNG

Der häufigste Fall einer Datensperre gemäss § 26 IDG ist die Sperrung der eigenen Daten bei der Einwohnergemeinde. Sie führt dazu, dass die Einwohnergemeinde die Daten nicht bekanntgeben darf, wenn z. B. eine Privatperson Auskunft über die Wohnadresse erhalten möchte. Hat jemand seine Daten im Sinne von § 26 Abs.1 IDG sperren lassen, ist zu prüfen, ob diese Datensperre allenfalls durchbrochen werden kann. § 26 Abs. 2 IDG listet die drei Voraussetzungen dafür auf: Entweder es liegt eine gesetzliche Verpflichtung des öffentlichen Organs zur Datenbekanntgabe vor, die Erfüllung einer gesetzlichen Aufgabe erfordert die Bekanntgabe oder die um Bekanntgabe ersuchende Person macht glaubhaft, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind. Dabei stellen sich im konkreten Einzelfall weitere Fragen, welche anhand zweier Fallbeispiele veranschaulicht werden sollen.

In der ersten Fallkonstellation wurde eine Gemeinde von einer Ausgleichkasse zur Herausgabe der Kontaktdaten einer Person angefragt, welche die Datensperre hinterlegt hatte. Die Gemeinde wandte sich somit mit der Frage an die ASD, ob die Datensperre im vorliegenden Fall durchbrochen werden könne.

Die Ausgleichkasse begründete ihr Gesuch damit, dass anhand des Zuzugsdatums des Kindes entschieden werde, ab wann die Kindsmutter berechtigt sei, Familienzulagen zu beziehen. Gemäss Familienzulagengesetz hat derjenige Elternteil Anrecht auf die Zulagen, bei welchem sich das Kind in Obhut befindet. In dieser Konstellation fungiert die Ausgleichskasse als Familienausgleichskasse. Mit § 8 Abs. 4 des Einführungsgesetzes zum Bundesgesetz über die Familienzulagen (SGS 838) besteht eine gesetzliche Grundlage, welche die Gemeinden dazu verpflichtet, *«den zugelassenen Familienausgleichskassen kostenlos alle für die Durchführung des Gesetzes erforderlichen Auskünfte zu geben»*. Die Gemeinde muss also der Ausgleichskasse die erwünschte Auskunft geben. § 26 Abs. 2 Bst. a IDG ist einschlägig – die von der betroffenen Person hinterlegte Datensperre wird dadurch durchbrochen.

In der zweiten Fallvariante gelangte eine Gemeinde (Zuzugsgemeinde) an die ASD, weil sie von einer anderen Gemeinde (Wegzugsgemeinde) nach der Adresse einer umgezogenen Privatperson angefragt wurde. Als die Person noch in der Wegzugsgemeinde wohnte, hatte sie eine Datensperre errichten lassen. Es stellt sich die Frage, ob die betreffende Person die Datensperre am neuen Ort bewusst nicht hatte errichten lassen oder nicht wusste, dass die Datensperre beim kantonsinternen Umzug nicht automatisch übernommen wird. Die bei der Wegzugsgemeinde anfragende Person war eine Verwandte der betroffenen Person, die den Kontakt zu ihr suchte. Aufgrund der speziellen Konstellation schlug die ASD der Gemeinde vor, die betroffene Person anzuhören. Zugleich konnte so auch geklärt werden, ob die Person die Errichtung einer Datensperre in der neuen Gemeinde wünschte. Folglich sah die ASD unter den gegebenen Umständen die Voraussetzungen einer Durchbrechung nach § 26 Abs. 2 IDG als nicht gegeben, insbesondere da nicht die Durchsetzung eines Rechtsanspruchs im Raume stand. Demnach darf die Bekanntgabe nur unter der Voraussetzung einer Zustimmung der betroffenen Person erfolgen.

2.10 WAS SIND «VORHANDENE» INFORMATIONEN?

Ein öffentliches Organ wandte sich mit der Frage an die ASD, was bei einem Zugangsgesuch zu Informationen unter dem Begriff «vorhandene» Informationen zu verstehen sei.

Mit der Einführung des Öffentlichkeitsprinzips 2013 erhielt jede Person das Recht auf Zugang zu Informationen, die beim öffentlichen Organ «vorhanden» sind. Die Frage, ob eine Information vorhanden sei, war Gegenstand einer Anfrage eines öffentlichen Organs an die ASD. Was bei den

öffentlichen Organen an Informationen vorhanden ist und vor allem in welcher Form, ist für die Bevölkerung nicht einfach herauszufinden. Die Person, die ein Zugangsgesuch stellt, hat jedoch die Pflicht, alle zumutbaren Angaben zu machen, die es dem öffentlichen Organ erlauben, das gewünschte Dokument zu identifizieren. Bei Unklarheiten kann das öffentliche Organ auch eine Präzisierung des Gesuchs verlangen (§ 20 Abs. 3 und 5 IDV). Durch diese Bestimmungen sowie die Voraussetzung, dass ein Dokument in irgendeiner Form vorhanden sein muss, soll vermieden werden, dass mittels eines Gesuches ein öffentliches Organ eine noch nicht vorhandene Information erstellen oder aufwändig nach vorhandenen Informationen suchen muss. Da aber das öffentliche Organ stets besser weiss, was bei ihm vorhanden ist, hat die Rechtsprechung für beide Fälle gewisse Mitwirkungspflichten der öffentlichen Organe herausgeschält. Erstens fallen Informationen, die zwar noch nicht vorhanden sind, aber durch einen einfachen (elektronischen) Vorgang, also quasi auf «Knopfdruck» erstellt werden können, auch unter den Begriff der vorhandenen Informationen. Im Falle eines Gesuches, in welchem verlangt wurde, dass das öffentliche Organ aus Daten, die bei ihm vorhanden waren, eine Statistik erstelle, hatte das Bundesgericht dies jedoch verneint (BGE 144 I 170, E. 8.3). Und zweitens trifft das öffentliche Organ insbesondere bei umfangreichen Gesuchen die Pflicht, bei der Präzisierung des Gesuches der gesuchstellenden Person zu helfen (BGE 142 II 324, E. 3.5).

Diese Präzisierungen machen aus Sicht der ASD auch für den Kanton Basel-Landschaft Sinn. Es gilt stets im Einzelfall Lösungen zu finden, die berücksichtigen, dass die gesuchstellende Partei einen Informationsrückstand hat. Demnach bekundet sie oftmals Mühe, ein Dokument genau zu bezeichnen, ohne andererseits das legitime Interesse des öffentlichen Organs an einer Einschränkung des Aufwands zu vernachlässigen. Aus diesem Grund empfiehlt es sich, mit dem Gesuchsteller oder der Gesuchstellerin frühzeitig den Dialog zu suchen.

2.11 WEM GEHÖRT DER BERICHT ÜBER DIE AUSWERTUNGEN EINES ASSESSMENTS?

Die ASD wurde angefragt, ob der Auswertungsbericht eines Assessments in einem Bewerbungsverfahren der Arbeitgeberin oder dem Bewerber gehöre, bzw. ob der Bewerbende Anspruch auf den vollständigen Bericht habe.

Die rechtlichen Grundlagen für die Bearbeitung der Daten zu Personen, die sich beim Kanton bewerben oder dort arbeiten, finden sich im Personalrecht, insbesondere im Personalgesetz (SGS 150) und in der Verordnung über den Umgang mit Personaldaten (SGS 150.21). Nach § 10 Personalgesetz dürfen die Personendaten von Stellenbewerberinnen und Stellenbewerbern bearbeitet werden, welche zur Beurteilung der Eignung notwendig und geeignet sind. Im zu beurteilenden Fall hatte der Arbeitgeber gestützt auf diese Bestimmung ein externes Unternehmen mit der Durchführung eines Assessments beauftragt. Das Unternehmen hatte daraufhin einen Bericht erstellt und dem Arbeitgeber übergeben. Der Bericht stellt somit eine Datenbearbeitung eines öffentlichen Organs für die Erfüllung seiner öffentlichen Aufgabe dar. Die ASD hielt darauf basierend fest, dass der durch das öffentliche Organ in Auftrag gegebene Bericht diesem gehöre.

Dies bedeutet jedoch nicht, dass die Person, die sich um die Stelle beworben hatte, keinen Anspruch darauf hat, den Bericht einzusehen und gegebenenfalls eine Kopie zu verlangen. Denn dieser Anspruch auf Zugang zu den eigenen Personendaten ist in § 24 IDG verankert und betrifft sämtliche Informationen, die über eine Person bei einem öffentlichen Organ vorhanden sind. Das Recht besteht grundsätzlich voraussetzungslos. Allerdings muss – wie bei jedem Fall einer Bekanntgabe von Personendaten – geprüft werden, ob allfällige überwiegende öffentliche oder private Interessen dem Zugang entgegenstehen könnten. Am Zugangsrecht ändert auch nichts, dass in der Verordnung über den Umgang mit den Personaldaten die Einsichtnahme durch Stellenbewerber – anders als durch Mitarbeitende – nicht ausdrücklich geregelt wird. Für Daten von Personen, deren Bewerbung nicht erfolgreich verläuft, sieht die Verordnung zudem eine Pflicht zur Rückgabe innert kurzer Frist bzw. die Vernichtung der Bewerbungsunterlagen vor, vorbehältlich besonderer Absprachen.

2.12 AUFFORDERUNG ZUR EINREICHUNG EINES ARBEITSVERTRAGS

Eine Privatperson kontaktierte die ASD und wunderte sich darüber, dass eine externe Dienstleisterin der Regionalen Arbeitsvermittlung (RAV) von ihr eine Kopie des Arbeitsvertrages ihrer neuer Stelle einforderte. Die Dienstleisterin

hätte ihr gegenüber erklärt, dass dies zwingend sei und sie den Vertrag sonst auch direkt vom RAV erhalten könne. Die ASD kontaktierte daraufhin das Unternehmen, welches im Auftrag der RAV Beratungs- und Wiedereingliederungsdienstleistungen erbringt, und wollte wissen, zu welchem Zweck der Vertrag eingefordert wurde. Es stellte sich heraus, dass der Zweck einzig darin bestand, den Fall ordentlich abschliessen zu können, da die betroffene Person eine neue Stelle gefunden hatte. Zu diesem Zweck ist allerdings lediglich eine entsprechende Bestätigung notwendig, nicht aber der gesamte Vertrag, welcher eine Vielzahl weiterer Daten enthält. Die ASD teilte dies sowohl der RAV als auch der Dienstleisterin mit und die entsprechenden Prozesse wurden daraufhin angepasst.

2.13 ZUGRIFF AUF NUTZUNGSDATEN VON SCHUL-TABLETS

Die kantonale Bildungs-, Kultur- und Sportdirektion (BKSD) hatte Mitte Jahr die Sekundarschülerinnen und -schüler mit Tablets ausgerüstet. Die «Basler Zeitung» griff dieses Thema am 11. August 2020 auf, wobei diverse Aussagen der BKSD zitiert wurden. Unter anderem wurde darüber informiert, dass gewisse Mitarbeitende beobachten könnten, wann ein Gerät eingeschaltet sei und welche Apps verwendet würden. Eine Privatperson wandte sich daraufhin an die ASD und wollte wissen, wie weit die diesbezüglichen Möglichkeiten der BKSD gingen und ob diese rechtmässig seien. Im weiteren Verlauf der Abklärungen wies die anfragende Person zudem auf die von der Schule erlassenen Nutzungsbedingungen hin, welche in wesentlichen Punkten von Vorgaben im auf den Tablets vorinstallierten BKSD-Handbuch abwichen.

Im Zuge der Abklärungen stellte sich heraus, dass die BKSD keinen Zugriff auf die Inhaltsdaten der auf den Geräten installierten Apps hat. Hingegen können die Mitarbeitenden gerätespezifische Informationen wie z. B. die Betriebssystemversion, die letzte Anmeldung an den Server und installierte Apps einsehen. Zudem kann die BKSD zum Zweck des sicheren und rechtmässigen Betriebs und Einsatzes im Bildungsbereich auf den Geräten eine Fernwartung durchführen. So können Geräte, die in den «Verloren-Modus» gesetzt wurden, geortet werden. Für die Bearbeitung von Daten der Schülerinnen und Schüler im Bildungsbereich zum Zweck der Organisation und Administration besteht mit § 4 a Abs. 1 Bst. a des Bildungsgesetzes (SGS 640) eine Rechtsgrundlage. Diese ist allerdings sehr allgemein gehalten. Angesichts der Tatsache, dass keine inhaltlichen Daten über die Nutzung erfasst wurden, schätzte die ASD die rechtliche Grundlage als knapp genügend ein.

Eine wichtige Frage stellte sich bezüglich der Verantwortung für die Geräte. Wenn die BKSD die Geräte an die Sekundarschülerinnen und Schüler verteilt, ist sie auch verantwortlich für die Ergreifung von angemessenen Schutzmassnahmen (§ 8 Abs. 1 IDG). Die BKSD konnte der ASD gegenüber darlegen, dass die Bearbeitungsmöglichkeiten alle dem Zweck dienten, sicherzustellen, dass die Geräte durch die Benutzenden rechtmässig verwendet werden (gesteuert beispielsweise über die Auswahl der Apps oder durch einen Content-Filter), dass allfällige Verstösse nachverfolgt werden können und dass die Geräte technisch auf dem neuesten Stand und im Notfall auffindbar sind.

Da die Datenbearbeitung durch die Benutzenden nach der Auslieferung der Tablets auf Weisung der Schulen (und nicht der BKSD) erfolgt, ist es wichtig, dass die BKSD die Schulleitungen ausreichend informiert und instruiert. Die schulspezifischen Weisungen sollten nicht den einzelnen Schulen überlassen werden, da sonst die BKSD ihre Verantwortung nicht wahrnehmen kann. Die ASD wies die involvierten Stellen auf diesen Umstand hin.

Ganz generell ist zu sagen, dass der Bildungsbereich gegenwärtig einen intensiven Digitalisierungsschub erfährt – auch unabhängig von den Covid-Massnahmen. Da im Bildungsbereich eine sehr grosse Anzahl Akteure mit einer noch grösseren Menge an zum Teil sehr sensitiven Personendaten arbeitet, stellen sich regelmässig komplexe datenschutzrechtliche Fragen. Die ASD steht diesbezüglich in Kontakt mit den Verantwortlichen und muss davon ausgehen können, dass neben den unzweifelhaft vorhandenen Chancen auch die Risiken erkannt und mit angemessenen Massnahmen begrenzt werden.

3 VORABKONTROLLE

Die Vorabkontrolle wurde 2008 als präventives Instrument gesetzlich verankert. Im Rahmen des Prüfprozesses 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. Durch «Privacy by Design» und «Privacy by Default» können entsprechende Risiken bereits in den frühen Phasen des Projektes eingeschätzt und mit geeigneten Massnahmen reduziert werden. *Im Nachhinein können Anforderungen an Datenschutz und Informationssicherheit oft nur noch mit grossen Mehrkosten oder im schlimmsten Fall gar nicht mehr erfüllt werden. Mit deren frühzeitiger Berücksichtigung lässt sich der Aufwand für eine datenschutzkonforme Lösung verringern.*

Nachdem die ASD 2014 eine IT-Revisionsstelle besetzen konnte, publizierte sie 2015 einen Leitfaden, welcher sowohl den Projektverantwortlichen als auch den verantwortlichen Organen als Unterstützung bei der Triage und Einbettung der Vorabkontrolle in den Projektablauf dient. Mit dieser Einbettung der Vorabkontrolle in bestehende Projektmethoden registriert die ASD eine markante Zunahme von ihr zur Vorabkontrolle vorgelegten Projekten.

Die datenschutzrechtlich zu prüfenden Angaben und Dokumente müssen nie ausschliesslich für diese Vorabkontrolle erarbeitet werden. Vielmehr sind sie wesentliche Bestandteile eines geordneten Projektmanagements, sollten im Laufe eines Informatikprojektes ohnehin erstellt werden und dienen danach einem geordneten und ausreichend sicheren Betrieb der Informatiklösung.

Die ASD prüft längst nicht alle Projekte, die ihr zur Vorabkontrolle vorgelegt werden. Eine erste grundsätzliche Beurteilung nimmt sie aufgrund einer Checkliste vor, die sie vom öffentlichen Organ ausfüllen lässt. Darauf basierend erfolgt die weitere Triage mittels einer erweiterten Risikobeurteilung. Seit 2014 wurde so bei 47 von 123 zur Vorabkontrolle eingereichten Projekten eine Vorabkontrolle durchgeführt. Bei 46 wurde aufgrund einer vertieften Risikobetrachtung auf die Durchführung einer Vorabkontrolle verzichtet. In vielen Fällen weist die ASD auch bei Verzicht auf eine Kontrolle auf im jeweiligen Kontext speziell zu beachtende Aspekte hin und steht bei konkreten Fragen beratend zur Verfügung.

Insgesamt wurden der ASD seit 2015 13 Projekte zu spät eingereicht, als dass ihre Empfehlungen noch eine Wirkung hätten erzielen können. Die ASD verzichtete in der Folge auf eine Durchführung der Vorabkontrolle. Zudem verzeichnete die ASD bis 2016 13 Projekte, die von den Verantwortlichen zwar rechtzeitig vorlegt wurden und bei denen der Prozess der Vorabkontrolle gestartet wurde, die Umsetzung jedoch bereits vor dem Erhalt der Stellungnahme der ASD begann und in der Folge die Empfehlungen nicht mehr berücksichtigt werden konnten. In den folgenden Jahren trat diese Art des Abbruchs der laufenden Vorabkontrolle nur noch selten auf.

Die der ASD zur Vorabkontrolle vorgelegten Projekte unterscheiden sich bezüglich Tragweite, Komplexität, eingesetzter Technologie und damit verbundenen Risiken stark voneinander. Die ASD hält die Durchlaufzeiten durchwegs so kurz wie möglich. Deshalb empfiehlt sie gerade bei grösseren Projekten eine möglichst frühe Kontaktaufnahme und bietet die iterative Durchführung des Prüfprozesses in mehreren und dafür kleineren Einzelschritten an. Komplexe Projekte – v. a. jene mit Rechtsetzungsbedarf – erstrecken sich teilweise über mehrere Jahre. Entsprechend dehnt sich auch der Zeitraum für die iterative Vorabkontrolle der einzelnen Projektdokumente.

Bei Projekten der kantonalen Verwaltung kann der Aufwand dank der guten und frühen Einbindung der jeweiligen Sicherheitsbeauftragten und der Rechtsdienste der Direktionen, welche die Informationseignerinnen bei der Wahrnehmung ihrer Verantwortung unterstützen, für alle Beteiligten kleiner gehalten werden. Die Erarbeitung von kantonalen Standards und Methoden, bei der die ASD mitwirken konnte, trägt mit der wachsenden Erfahrung der Sicherheitsbeauftragten und Projektleitenden dazu bei, dass der Aufwand pro Vorhaben für Behörden und ASD abnimmt. Einen Beitrag dazu leistet u. a. die kürzlich erstellte Checkliste betreffend Anforderungen an Cloud-Lösungen.

Im Berichtsjahr sind 31 Projekte neu eingegangen, zu neun davon hat die ASD keine Vorabkontrolle durchgeführt, neun Vorabkontrollen konnten abgeschlossen werden.

Bei den der ASD vorgelegten Projekten waren auch Cloud-Lösungen vertreten. Im Rahmen der Evaluierung der Cloud-Lösung eines weltweit tätigen Anbieters gab das verant-

wortliche öffentliche Organ ein Rechtsgutachten in Auftrag. Das Gutachten hatte zum Ziel, allfällige rechtliche Vorbehalte gegenüber einer Auslagerung nach § 7 Abs. 1 Bst. a IDG zu identifizieren. Das externe Rechtsgutachten wies aus, dass dieser Auftragsdatenbearbeitung keine zwingenden rechtlichen Hindernisse entgegenstehen. Da die Prüfung der Angemessenheit der vom Anbieter vertraglich zugesicherten und getroffenen Massnahmen i. S. v. § 8 IDG nicht Gegenstand des Gutachtens war, musste diese im weiteren Verlauf überprüft werden.

Die Vorabkontrolle ergab, dass die verbleibenden Restrisiken unter Berücksichtigung des Schutzbedarfs der für die Bearbeitung vorgesehenen Informationen zu hoch waren. Auch wenn im vorliegenden Fall die Informationen in einem Land mit vergleichbarem Datenschutzniveau bearbeitet werden, waren die Massnahmen für streng vertrauliche Informationen insbesondere bezüglich der gewählten Verschlüsselungsart, des Nachweises der Angemessenheit der Schutzmassnahmen sowie der vertraglichen Einsichtsrechte in die Zugriffsprotokolle durch das verantwortliche öffentliche Organ nicht angemessen.

Um das Schadensausmass und somit das Risiko zu minimieren, wurden zusätzlich organisatorische Massnahmen getroffen: Bis zur Anpassung der Schutzmassnahmen durch die Anbieterin dürfen gemäss Weisung des verantwortlichen öffentlichen Organs nur vertrauliche statt streng vertrauliche Informationen in der Applikation bewirtschaftet werden. Da organisatorische Massnahmen Risiken weniger stark minimieren als technische, verbleiben auch so erhöhte Restrisiken. Die ASD empfahl dem öffentlichen Organ, die Cloud-Lösung aufgrund der verbleibenden Restrisiken angesichts der verwaltungsweiten Verbreitung durch den Regierungsrat akzeptieren zu lassen.

4
KONTROLLTÄTIGKEIT

Gemäss § 40 lit. a IDG kontrolliert die Aufsichtsstelle Datenschutz nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen. Im Rahmen dieser datenschutzrechtlichen Kontrollen prüft die ASD die Umsetzung der rechtlichen, organisatorischen und technischen Vorgaben. Grundlage dafür bilden die eingereichten Unterlagen, Stichproben der erfolgten Zugriffe, Interviews mit den Verantwortlichen sowie die vor Ort festgestellten Massnahmen. Anders als bei der präventiven Vorabkontrolle während der Konzeption wird hier die Einhaltung der Vorgaben im laufenden Betrieb geprüft. Die ASD 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.

SCHENGEN-KONTROLLE

Die kantonalen Datenschutzbeauftragten sind gehalten, die Rechtmässigkeit der Bearbeitung personenbezogener Daten im Schengener Informationssystem (SIS) periodisch zu kontrollieren (Art. 60 Beschluss 2007/533/JI bzw. Art. 44 Verordnung (EG) 1987/2006 sowie Art. 55 Abs. 1 N-SIS-Verordnung). Die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft (ASD) führte im Dezember 2019 im Rah-

men einer Schengen-Kontrolle eine Datenschutzprüfung beim Amt für Migration und Bürgerrecht (AFMB) durch. Die Auswertung der Prüfung und der Bericht erfolgten im Berichtsjahr.

Die ASD stellte fest, dass die Nutzung des Schengener Informationssystems (SIS) bzw. der nationalen Informationssysteme in den Bereichen des AFMB unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgt. Im Rahmen der Stichprobenkontrolle konnten die Abfragen mit der Aufgabenerfüllung der fraglichen Personen begründet und anhand der entsprechenden Papier-Dossiers oder Einträge in der elektronischen Geschäftskontrolle erläutert werden. Einzelne Abfragen wurden durch eine Verkettung der Abfrage eines anderen Bundessystems mit dem SIS automatisiert ausgelöst.

Die befragten Mitarbeitenden des AFMB sind sich der Sensitivität der von ihnen bearbeiteten Personendaten bewusst. Das SIS selbst wird technisch und organisatorisch durch Informationssicherheitsmassnahmen geschützt. Die ASD prüfte ergänzend zu den Logfile-Kontrollen die Einhaltung gewisser organisatorischer Grundschutzmassnahmen bezüglich Informationssicherheit vor Ort und gab drei Empfehlungen für einen verbesserten Schutz ab.

KLINIK ARLESHEIM

Aus datenschutzrechtlicher Sicht vereinen die Tätigkeiten der Klinik Arlesheim verschiedene Risiken für die Rechte und Freiheiten der Betroffenen: In der Klinik werden besondere Personendaten sowie Persönlichkeitsprofile im Sinne von § 3 Abs. 4 Bst. a und b IDG bearbeitet, was grundsätzlich ein hohes Datenschutzrisiko bedeutet. Weitere Risiken ergeben sich aus der Vielzahl an Schnittstellen und der damit verbundenen häufigen Bekanntgabe von Personendaten infolge der interdisziplinären Zusammenarbeit mit anderen Stellen sowie Personen. Die Datenbearbeitung durch Outsourcing-Partner ist erfahrungsgemäss mit zusätzlichen Risiken verbunden. Zudem ist eine grosse Anzahl von Personen von der Datenbearbeitung betroffen. Deshalb wurde die Klinik Arlesheim per Ende 2019 für eine Kontrolle ausgewählt.

Die Datenschutzprüfung wurde schwerpunktmässig in zwei Kontrollbereiche unterteilt: Zum einen untersuchte die ASD Vorgaben und Massnahmen, die für einen datenschutz- und informationssicherheitskonformen Betrieb der IT-Infrastruktur relevant sind. Zum anderen prüfte sie die Datenbearbeitung von Patientendaten im Klinik-Informationssystem (KIS).

Bei allen an der Prüfung Beteiligten war eine hohe Sensibilisierung für die Themen Datenschutz und Informationssicherheit vorhanden. Dennoch deckte die Prüfung verschiedene organisatorische wie technische Schwachstellen auf. In den organisatorischen Bereich fallen u. a. unzureichende Vereinbarungen mit Auftragnehmerinnen. Empfehlungen sprach die ASD auch bezüglich der Verwendung von privaten mobilen Geräten für den Zugriff auf die Daten der Klinik aus. Ausserdem war die Umsetzung des Datenlebenszyklus in Verbindung mit einer Änderung der Zugriffsrechte bei der elektronischen Datenbearbeitung nicht angemessen.

CORONABEDINGT VERSCHOBENE PRÜFUNGEN

Aufgrund der vom Bundesrat und Regierungsrat des Kantons Basel-Landschaft beschlossenen Massnahmen gegen die Ausbreitung des Corona-Virus entschied der Datenschutzbeauftragte, zwei Vor-Ort-Prüfungen auf die Zeit nach diesen Massnahmen zu verschieben. Eine absolute Notwendigkeit, die Prüfung unter diesen Umständen vor Ort durchzuführen, lag nicht vor und die ASD wollte eine unnötige Gefährdung der Beteiligten ausschliessen. Eine digitale Durchführung ist bei den ausgewählten öffentlichen Organen unter diesen Umständen nicht geeignet und birgt unnötige Prüfrisiken.

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 2019	**Gesuche 2020**	gutgeheissen	teilweise gutgeheissen	abgewiesen
BKSD	0	**2**	2	0	0
BUD	3	**1**	1	0	0
FKD	0	**1**	0	0	1
SID	4	**8**	8	0	0
VGD	8	**7**	3	2	2
LKA	13	**4**	2	1	1
Total	**28**	**23**	**16**	**3**	**4**

Die Zahlen weisen ein insgesamt ungefähr gleichbleibendes Niveau aus, wobei die Sicherheitsdirektion deutlich mehr, die Landeskanzlei, welche auch für Zugangsgesuche zu Informationen des Regierungsrats zuständig ist, deutlich weniger Gesuche zu verzeichnen hatte. Die Zunahme von Gesuchen im Zuständigkeitsbereich der Sicherheitsdirektion erklärt sich fast vollständig aus der Tatsache, dass dort der Kantonale Krisenstab (KKS) angesiedelt ist, der sich auch mit der Bewältigung der Pandemie beschäftigt.

Da die Gemeinden eingegangene Gesuche nicht melden müssen, kann die ASD nur aufgrund der erhaltenen Beratungsanfragen abschätzen, ob sich die Gesuchszahlen spürbar verändert haben. Dies scheint jedoch nicht der Fall zu sein. Die ASD hatte betreffend Zugangsgesuche gegenüber 2019 nur unwesentlich mehr Anfragen von Behörden und etwas weniger Anfragen von Privaten.

Das Verbleiben der Zahlen auf einem relativ überschaubaren Niveau heisst indessen nicht, dass es in Einzelfällen nicht zu relativ komplexen Verfahren kommt. Sowohl das Verfahren wie auch die materielle Beurteilung der jeweils zu prüfenden Einschränkungs- und Verweigerungsgründe stellen die Rechtsdienste punktuell vor komplexe Fragestellungen. Sie scheinen dabei aber keineswegs überfordert, denn die Tatsache, dass das Kantonsgericht seit Bestehen des Öffentlichkeitsprinzips soweit ersichtlich erst einen Fall aus diesem Rechtsgebiet veröffentlich hat, deutet darauf hin, dass die Vorinstanzen zu Lösungen finden, die fundiert begründet und nachvollziehbar sind. Immerhin werden nach der Statistik der kantonalen Verwaltung über 80 % der Gesuche zumindest teilweise gutgeheissen.

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 einbringen. Im Berichtsjahr konnte die ASD in dieser Rolle nebst Beratung bei aktuellen Themen auch Unterstützung bei der Konzeption der neuen Passwortrichtlinien und bei der Anpassung der Schutzbedarfsanalyse bieten. Des Weiteren berichtete die ASD in der FIS über die häufigsten Feststellungen bei der Beurteilung von Risikoanalysen im Rahmen der Vorabkontrollen.

Die Sicherheitsbeauftragten und Projektleitenden des Kantons wünschten sich eine Konkretisierung des *privatim*-Merkblatts zu cloudspezifischen Risiken und Massnahmen, weil sich dieses nicht unmittelbar auf die Evaluierung von Cloud-Lösungen übertragen liess. Im konkreten Fall mussten die im Merkblatt aufgeführten Risiken bezogen auf die geplante Datenbearbeitung jeweils erst erkannt werden. Der kantonale Sicherheitsbeauftragte gelangte deshalb mit dem Anliegen an die ASD, die Inhalte des Merkblattes gemeinsam in Form eines Anforderungskatalogs zu konkretisieren.

Als Grundlage für die Anforderungen dienten nebst dem Cloud-Merkblatt von *privatim* die kantonalen Regelwerke, die AGB der Schweizerischen Informatikkonferenz (SIK) und europäische Frameworks.

Daraus entstand unter Beizug der ASD eine Checkliste, welche den Schutzbedarf der Informationen und Abhängigkeiten zwischen den Risiken berücksichtigt. Sie enthält die Minimalanforderungen bezüglich Informationssicherheit und Datenschutz bei Cloud-Lösungen, welche vermehrt Bestandteil neuer Services und der damit verbundenen Evaluation und ISDS-Konzepte sind. Die Checkliste entlastet die öffentlichen Organe spürbar bei den Abklärungen zu geplanten Cloud-Lösungen.

6.3 DATENSCHUTZBEHÖRDEN ANDERER KANTONE

Die Zusammenarbeit mit Datenschutzbehörden anderer Kantone ist für die ASD wichtig. Auch wenn die Kanton individuelle 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 in anderen Kantonen bereits im Einsatz sind. Dies wirkt sich positiv auf Qualität und 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. Insgesamt hat sich die ASD im Berichtsjahr bei 57 Geschäften mit anderen Aufsichtsbehörden ausgetauscht.

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.

Aufgrund der Covid-19-Situation war der Austausch in den *privatim*-Arbeitsgruppen nicht so intensiv wie in den Vorjahren. Ein schnellerer und weniger an Strukturen gebundener Austausch ausserhalb der Arbeitsgruppen wurde angesichts der anstehenden Themen intensiviert.

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 beim Austausch zu konkreten Projekten sowie kantonsübergreifenden Lösungen und Umsetzungen in den einzelnen Kantonen.

6.5 AG SICHERHEIT

Die AG Sicherheit hat zum Ziel, kantonsübergreifende Themen vornehmlich aus dem Bereich der Datenbearbeitungen durch die Polizei, aber etwa auch Strafvollzugs- oder Migrationsbehörden zu besprechen und allenfalls zu koordinieren.

Die ASD hat die Leitung dieser Gruppe übernommen. Im Berichtsjahr traf sich die AG coronabedingt lediglich einmal. Zur Sprache kam eine Reihe von aktuellen Projekten, thematisiert wurden aber auch technologische Entwicklungen, die sich zwar abzeichnen, aber noch etwas weiter in der Zukunft liegen.

Ausserhalb der Sitzung befasste sich eine Untergruppe mit der Koordination der Formulierung datenschutzrechtlicher Aspekte im Bereich des «Electronic Monitoring».

6.6 AG GESUNDHEIT

Das Berichtsjahr war für die AG Gesundheit aus nachvollziehbaren Gründen besonders intensiv. Die Situation um die Corona-Pandemie erforderte eine deutlich höhere Sitzungskadenz, da der Bedarf an Austausch und Koordination unter den Kantonen angesichts der teils sehr raschen Entwicklung sehr hoch war und auch vorerst bleibt. Fragen rund ums Testen, Contact Tracing sowie Impfungen dominierten die Agenda. Dabei zeigte sich auch, dass ad hoc kleinere Gruppen gebildet werden mussten, da in den Kantonen oft mit verschiedenen Informatik-Lösungen gearbeitet wird, welche jeweils unterschiedliche Fragen aufwerfen.

6.7 AG-DIGITALE VERWALTUNG

Die AG Digitale Verwaltung traf sich im Berichtsjahr nur einmal. Sie beschäftigte sich primär mit der Umsetzung der Meldepflicht von Datenschutzvorfällen («Data Breaches»).

6.8 KOORDINATIONSGRUPPE ZUM SCHENGENER INFORMATIONSSYSTEM (SIS)

Die SIS-Koordinationsgruppe führte im Berichtsjahr keine Sitzungen durch. Sie wurde von der Vertreterin des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auf schriftlichem Weg über die primär auf europäischer Ebene erfolgten Entwicklungen auf dem Laufenden gehalten.

Über diese institutionalisierten Arbeitsgruppen hinaus bilden sich beispielsweise für Vertrags- oder Systemprüfungen von in mehreren Kantonen eingesetzten Informatiklösungen jeweils Ad-hoc-Arbeitsgruppen mit *privatim*-Delegierten.

7
SCHULUNGEN UND REFERATE

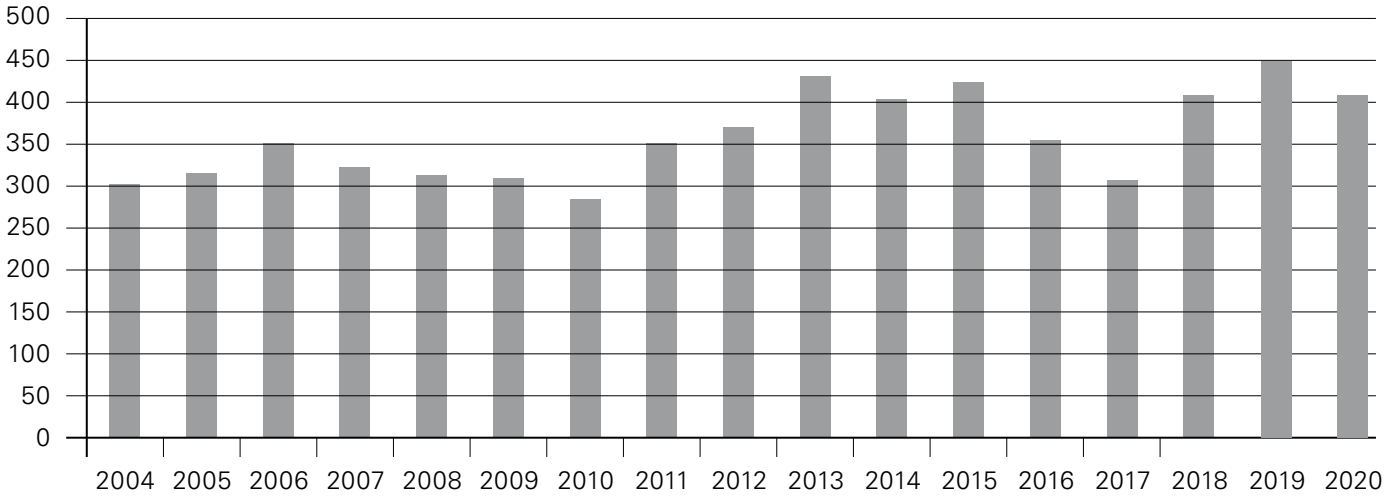
Die Schulungen und Referate der ASD sollen die Teilnehmenden für die Themen Datenschutz und/oder Informationssicherheit sensibilisieren und sie dazu befähigen, Aufgaben und Fragestellungen in diesem Bereich besser und somit auch effizienter zu bewältigen. Sie sind geeignete Werkzeuge für die Stärkung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

Auch in diesem Berichtsjahr hat die Aufsichtsstelle Datenschutz die jährlich wiederkehrenden Schulungen durchgeführt, wie z. B. bei den Lernenden der kantonalen Verwaltung und den Polizeiaspirantinnen und -aspiranten. Auch die Kurse des Personalamtes zum Thema Datenschutz und Öffentlichkeitsprinzip konnten fast vollständig durchgeführt werden. Natürlich waren auch hier die Auswirkungen der Pandemie zu spüren, sodass ein Teil der Referate virtuell stattfinden musste. Die ASD bedankt sich bei dieser Gelegenheit bei den Organisatoren für ihre Unterstützung.

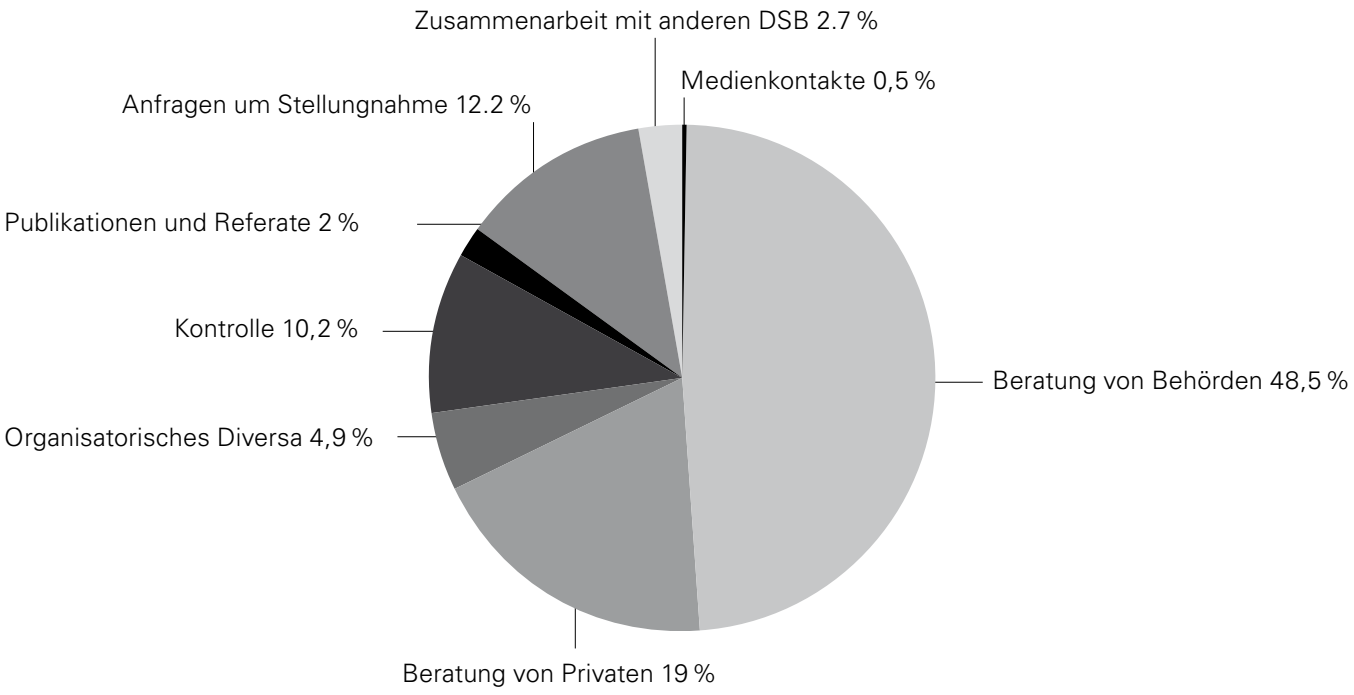
Etwas in den Hintergrund traten die themenspezifischen Referate. So fiel etwa ein Referat bei der KESB dem Virus zum Opfer. Es zeichnet sich aber schon jetzt ab, dass die Anzahl der Schulungen und Referate im nächsten Jahr eher zunehmen könnte. Dies ist nicht nur einem gewissen Nachholeffekt geschuldet, sondern ergibt sich auch durch die Revision des IDG.

8 ANHANG

8.1 ANZAHL NEU ERÖFFNETE GESCHÄFTE



8.2 ART DER GESCHÄFTE



(Basis: Anzahl Geschäftsfälle)