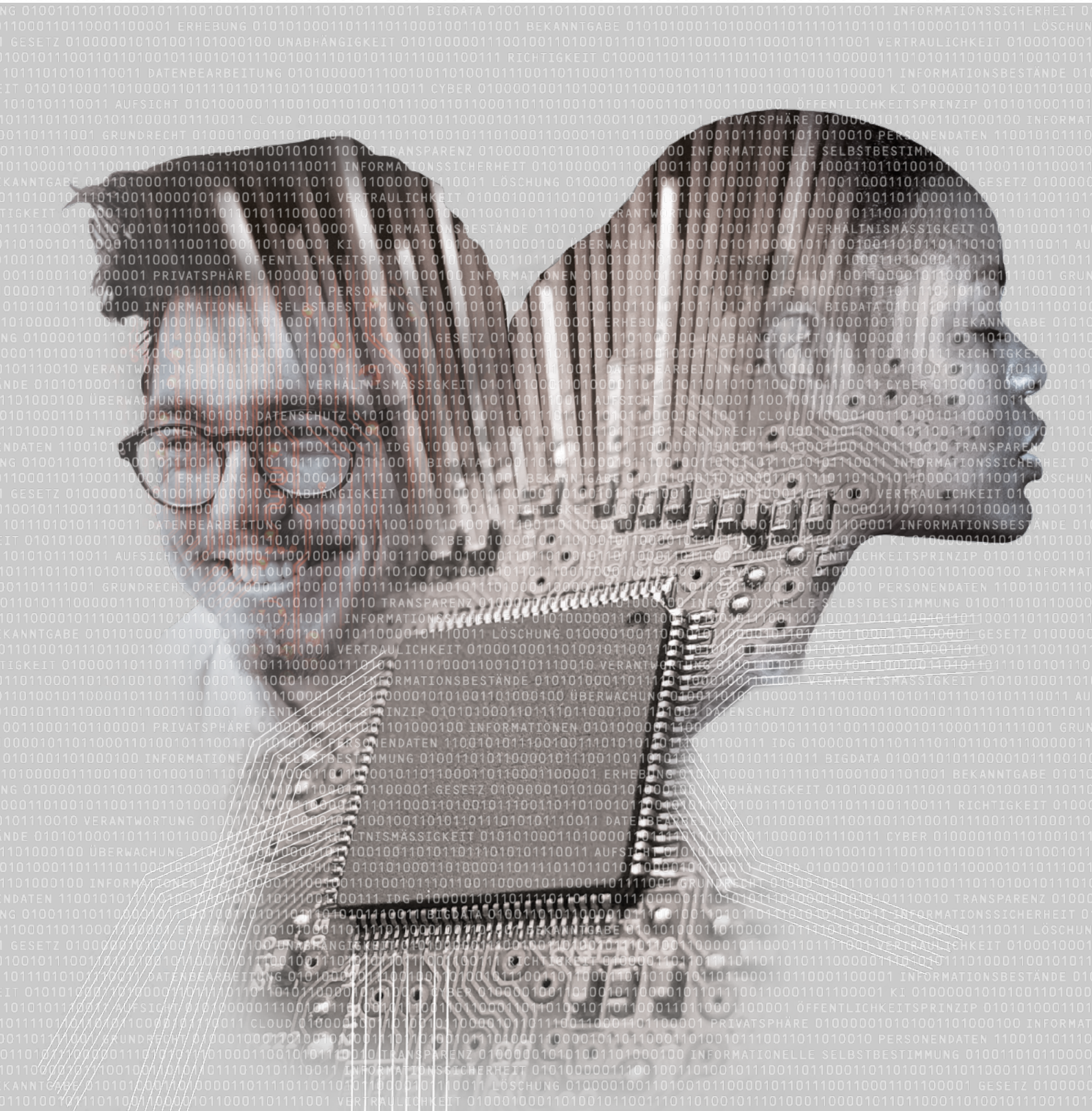
BASEL LANDSCHAFT

TÄTIGKEITSBERICHT 2021
DER AUFSICHTSSTELLE DATENSCHUTZ



AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragter:
Markus Brönnimann

Stv. Datenschutzbeauftragte:
Priscilla Dipner-Gerber
Thomas Held

Akademische Mitarbeitende:
Ditmar Freitag
Simon Habermacher
Beate Metz

Büro:
Kanonengasse 20
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 2021

1.1 DIE AUFSICHTSSTELLE DATENSCHUTZ (ASD)

Die ASD ist eine unabhängige Aufsichtsbehörde. Sie verfügt über fundiertes Fachwissen bezüglich Datenschutz, dem Umgang mit Informationen, Informationssicherheit und Governance. 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. Ihr Angebot umfasste auch Auskünfte an und fachlich fundierte Einschätzungen für Landrat und Medien.

Im Berichtsjahr hat die ASD 383 Dossiers eröffnet. Der Aufsichtsstelle wurden 36 neue Vorhaben zur Vorabkontrolle vorgelegt. Bei 13 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, 172 Beratungen bei öffentlichen Organen und 68 bei Privatpersonen durchgeführt sowie zehn Schulungen und Referate gehalten. Die ASD wurde für 54 Stellungnahmen angefragt und verfasste weitere 47 Stellungnahmen im Rahmen von Vorabkontrollen. Bei 67 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 Frau Evi Karapetsa und Herr Jonas Stettler die ASD tatkräftig im Rahmen des jeweils sechsmonatigen Volontariates für Juristen und Juristinnen, welches die ASD auch im Berichtsjahr anbot.

1.2 COVID

2021 war das zweite von der Covid-Pandemie geprägte Jahr. Eine Herausforderung für den Datenschutz stellte das Spannungsfeld dar zwischen dem Recht jeder Person auf Schutz ihrer Privatsphäre und der Pflicht von Bund und Kantonen, dieselbe Person vor der Pandemie zu schützen. Massnahmen zur Eindämmung der Pandemie hatten oft eine grundsätzliche Einschränkung der Freiheiten für die Einwohnerinnen und Einwohner der ganzen Schweiz bzw. einzelner Kantone zur Folge. In der Regel zogen solche Massnahmen teils umfangreiche Datenbearbeitungen nach sich. Die Beurteilung von deren Rechtmässigkeit war somit stets eng verknüpft mit der Beurteilung der Verfassungsmässigkeit der Massnahmen selbst. Dabei bestand für den Gesetzgeber sowie die Rechtsanwender die besondere Herausforderung, dass sich die rechtlichen Grundlagen sowohl auf Bundesebene als auch in den Kantonen in einem atemberaubenden Tempo änderten. Zudem war die Rechtsprechung zu beachten, die sich wiederholt zu den Massnahmen äusserte. Grundsätzlich richtete sich die Gestaltung der Massnahmen nach den Vorgaben des Bundesgesetzes vom 28. September 2012 über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz, EpG). Hinzu kamen nun aber auch das Covid-Gesetz, zahlreiche Verordnungen sowie die kantonalen Covid-Regelungen. Deren Erlass erfolgte oft unter grossem Druck. In der Folge mussten innert kürzester Zeit die entsprechenden Massnahmen ergriffen und Lösungen evaluiert sowie umgesetzt werden. Auf detaillierte Abklärungen musste teilweise verzichtet werden, was mitunter auch zum Einsatz von zu wenig sicheren Lösungen führte. Die Exekutivbehörden waren gefordert, möglichst rasch Lösungen von möglichst hoher Qualität zu finden; die Aufsichtsbehörden mussten – sofern sie involviert wurden – diese unter ebenso hohem Zeitdruck beurteilen. Dies band eine erhebliche Menge an Ressourcen.

Ein zentrales Element der Pandemie waren zudem die langen Phasen der eingeschränkten physischen Präsenz am Arbeitsplatz und an den Schulen. Innert kürzester Zeit mussten umfangreiche Lösungen für Fernunterricht und Homeoffice oder aber Schutzmassnahmen für das Arbeiten vor Ort gefunden und umgesetzt werden.

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

Bei der Umsetzung der Pandemie-Schutzmassnahmen und bei der Aufgabenerfüllung kam es vor, dass die für jede Datenbearbeitung erforderliche Interessen- und Risikoabwägung teilweise zu anderen Ergebnissen führte, als dies im Regelbetrieb der Fall gewesen wäre. Zur Erfüllung des schulischen Bildungsauftrags und der öffentlichen Aufgaben der Behörden mussten in dieser Zeit teilweise Lösungen eingesetzt werden, welche die Anforderungen an den Datenschutz und die Informationssicherheit (noch) nicht vollumfänglich erfüllten. Die eingesetzten Lösungen konnten entsprechend von den Datenschutzaufsichtsstellen bestenfalls summarisch geprüft werden.

Ausserordentliche Lagen verlangen nach ausserordentlichen Massnahmen. Nach der Normalisierung der Lage sollte nun aber im Sinne einer Nachbereitung dringend evaluiert werden, was sich bewährt hat und wo Nachbesserungsbedarf besteht. Die Aufteilung, was zentral vom Bund vorgegeben wird und was von den Kantonen verantwortet werden muss, sollte sowohl mit Bezug auf die Kompetenzen in der jeweiligen epidemiologischen Lage als auch hinsichtlich der Informationsbearbeitung kritisch hinterfragt werden. Geben beispielsweise Exekutivbehörden des Bundes Empfehlungen zum Einsatz von Applikationen ab, so sollte trotz aller Eile vorab geprüft worden sein, dass die Lösung den Anforderungen an den Datenschutz und die Informationssicherheit genügt. Im Falle von schweizweit geltenden Massnahmen sollte abgewogen werden, ob eine Zielvorgabe ausreicht oder ob es punktuell sinnvoller wäre, bereits konkrete IT-Lösungen und den Umfang der zu bearbeitenden Informationen abschliessend vorzugeben. Hierbei geht es nicht darum, die Kompetenzen der föderalen Ebenen auszuhebeln, sondern in einer Notlage so effizient und effektiv wie möglich mit überschaubaren Risiken zu agieren. Ohne ein solches Vorgehen entsteht den Kantonen trotz guter Absichten potenziell ein grösserer Mehraufwand. Die föderalistischen Strukturen wurden in der Pandemie auf eine harte Probe gestellt. Gerade im Bereich der Datenbearbeitungen führte dies dazu, dass gewisse Daten über denselben Sachverhalt in benachbarten Kantonen unterschiedlich bearbeitet werden mussten, da die rechtlichen Grundlagen nicht die gleichen waren oder unterschiedlich ausgelegt wurden. Eine solche Situation sollte aus Sicht der ASD möglichst vermieden werden.

Einen sorgfältigen Umgang braucht es auch mit den während der Pandemie etablierten Tools und Arbeitsweisen. Nur weil man sich während zwei Jahren an diese gewöhnt hat und bis anhin (noch) keine negativen Konsequenzen erkennbar sind, heisst dies nicht, dass man an ihnen festhalten muss. Hier erscheint es sinnvoll, die Anwendungen und Methoden, welche auch nach der Pandemie beibehalten werden sollen, bezüglich Rechtskonformität, Sicherheit, Nutzen und allfälligen Risiken zu untersuchen. Ziel muss es sein, die gewonnenen Erkenntnisse in stabile, zukunftsfähige Lösungen einfliessen zu lassen, damit die – zumindest was die Datenbearbeitung betrifft – durchaus vorhandenen positiven Impulse aus der Pandemie-Zeit übernommen werden können.

1.3 VISITATION GESCHÄFTSPRÜFUNGSKOMMISSION (GPK)

Im Rahmen ihres ordentlichen Besuchsprogramms führte die zuständige Subkommission (Subko IV) der Geschäftsprüfungskommission (GPK) im März des Berichtsjahres eine Visitation der ASD durch. In ihrem Bericht hält die GPK in Bezug auf die Digitalisierung und die Vorabkonsultation (Vorabkontrolle) unter anderem fest: *«Für eine im Gesetz vorgesehene Kontrolle und Beratung über die kantonale Verwaltung hinaus reichen die aktuellen 450 Stellenprozente nicht aus. Damit bleibt das Thema Datenschutz bei den Gemeinden, den anderen öffentlichen Organen und Privaten mit öffentlichen Aufgaben (wie Kantonsspital Baselland (KSBL), Spitex, Pflegeheime etc.) auf Standby und kann nicht proaktiv angegangen werden. Die Subko IV interessierte sich in diesem Zusammenhang für die Risikofrage: Letztlich muss jemand am Schluss das Risiko tragen, wenn die Informationssicherheit nicht voll gewährleistet ist. Die ASD arbeite auf das Ziel hin, dass ein öffentliches Organ jeweils das Risiko tragen kann. Die Unabhängigkeit der ASD böte in gewisser Weise die Gewähr, dass diese Risikoabschätzungen sachlich und fachlich neutral erfolgten.»*

FESTSTELLUNGEN

Die Subko IV stellte basierend auf ihrem Besuch fest, dass
- sich die ASD seit der letzten Visitation der GPK professionalisiert hat und im Rahmen ihrer personellen Möglichkeiten sehr strukturiert vorgeht.
- die Herausforderungen im juristischen und IT-Bereich sehr dynamisch und komplex sind.
- eine proaktive Bearbeitung von Fragen des Datenschutzes und der Informationssicherheit ausserhalb der kantonalen Verwaltung aus Kapazitätsgründen kaum stattfindet.
- ausserhalb de r kantonalen Verwaltung ein grosser Sensibilisierungsbedarf besteht.
- jeder Kanton i. d. R. alles (insbesondere IT-System) selber prüft.
- rasche IT-Lösungen, die aufgrund der Covid-19-Pandemie gewählt werden mussten, dem IDG auf Dauer mutmasslich nicht genügen.

Die Feststellungen sind für den Datenschutzbeauftragten nachvollziehbar und zutreffend.

EMPFEHLUNGEN

Im Rahmen ihrer Oberaufsicht empfiehlt die GPK der ASD:
- Die Zusammenarbeit mit den verschiedenen Datenschutzstellen anderer Kantone ist zu intensivieren (z. B. bei bereits geprüften IT-Applikationen, Erfahrungsaustausch zu juristischen Fallabklärungen).
- Die Sensibilisierungsarbeit bei den Gemeinden und externen öffentlichen Organen des Kantons, die ASD bei datenschutzrelevanten Projekten zu konsultieren, ist zu intensivieren.
- Nach der Covid-19-Pandemie weiterhin verwendete oder neue Remote-Working-Tools sind auf ihre IDG-Tauglichkeit zu überprüfen.

Die Empfehlungen der GPK sind verständlich und unterstützen die Gesamtausrichtung der Aufsichtsstelle Datenschutz. Der Datenschutzbeauftragte wird die drei empfohlenen Stossrichtungen im Rahmen der zur Verfügung stehenden Ressourcen weiterverfolgen.

RESSOURCEN

Der Datenschutzbeauftragte hatte bereits vor der Visitation der GPK aufgrund der kontinuierlich steigenden Anforderungen und der Bedeutung von Datenschutz und Informationssicherheit zusätzliche personelle Ressourcen per 2022 beantragt mit dem Ziel, seinen gesetzlichen Auftrag besser erfüllen zu können. Der Landrat hat der Erhöhung der personellen Ressourcen zugestimmt und unterstreicht damit, dass ihm Datenschutz und Informationssicherheit in einer zunehmend digitalisierten Gesellschaft in unserem Kanton wichtig sind.

AUSBLICK

In vielen Kantonen wurden die Budgets der Datenschutzbehörden in den vergangenen Jahren erhöht. Es bleibt zu hoffen, dass auch Kantone, die bis dato für den Datenschutz wenig Ressourcen aufwenden, zukünftig zusätzliche Mittel sprechen. Mit der zunehmenden Digitalisierung werden Lösungen vermehrt in mehreren oder gar allen Kantonen genutzt, Prozesse automatisiert sowie Informationen digital auf allen Ebenen ausgetauscht. Dies bedeutet eine grosse Herausforderung sowohl für die Exekutiven als auch die Datenschutzbehörden über alle drei föderalen Ebenen (Bund, Kantone und Gemeinden) bei rechtlichen, organisatorischen und technischen Fragen. Notwendig ist auch eine gesellschaftliche Diskussion zu Digitalisierung und Datenschutz. Die Exekutive und die Aufsichtsbehörden sind darauf angewiesen, dass diese Themen soweit als möglich aktiv gestaltet sowie Aufträge und Rahmenbedingungen in Form von Gesetzen möglichst klar vorgegeben werden.

Mit der immer grösser werdenden Abhängigkeit von IT-Systemen und digitalen Informationen sind weitere wichtige Themen im direkten oder indirekten Zusammenhang mit dem Datenschutz und der Informationssicherheit zu beurteilen. Hierunter fallen beispielsweise die (Daten-)Souveränität und die Unabhängigkeit von Lieferanten, die Zuverlässigkeit und Nachvollziehbarkeit von Algorithmen und von darauf basierenden Entscheidungen, freie und nicht manipulierte Meinungsbildung sowie das Verhältnis von Kosten/Nutzen und akzeptablen, nicht nur monetären Risiken. Zudem braucht es auch weiterhin ausreichend internes Fachwissen und Flexibilität, um den stetig sich verändernden Herausforderungen und Bedrohungslagen gerecht zu werden (z. B. Pandemie, Kriege und deren Folgen, exterritoriale Gesetzesänderungen, etc.).

Die Datenschutz-Aufsichtsbehörden können dazu mit ihrer gesetzlich garantierten Unabhängigkeit sowie dem breiten Fachwissen im Bereich Recht und Digitalisierung einen wesentlichen und parteipolitisch neutralen Beitrag leisten.

2

2 AUS DEM BERATUNGSALLTAG

2.1 AUSGESTALTUNG DES WAHLVERFAHRENS IN DEN GEMEINDEN

Die ASD wurde im Rahmen der Teilrevision des Gesetzes über die politischen Rechte (GpR, SGS 120) zur Stellungnahme bezüglich Wahlen und Abstimmungen eingeladen. Von Interesse waren die Bestimmungen zur Ausgestaltung des Stimmrechtsausweises und des Stimmrechtscouverts sowie insbesondere die Verpflichtung der Gemeinden, den Stimmberechtigten zur Wahrung des Stimmgeheimnisses nach § 7 Abs. 4 GpR einen zusätzlichen Umschlag für die Stimm- und Wahlzettel zuzustellen.

Die ASD kam zum Schluss, dass sich bei der Briefwahl ohne ein zusätzliches Couvert nicht ausschliessen lässt, dass der Stimm- und Wahlzettel mit der stimmberechtigten Person in Verbindung gebracht wird. Damit wäre die Anonymität nicht gegeben und das Stimmgeheimnis durchbrochen. Zudem stellt das Stimmgeheimnis nicht nur ein Recht der stimmberechtigten Person dar, sondern leitet sich daraus auch die Pflicht der öffentlichen Organe ab, organisatorische und technische Vorkehrungen zu treffen, welche die Geheimhaltung während des Wahl- und Stimmverfahrens sicherstellen. Die Pflicht des für eine Datenbearbeitung verantwortlichen Organs ergibt sich auch aus § 8 IDG. Bis die Stimmzettel von den Stimmrechtsausweisen getrennt werden (und damit eine Anonymisierung stattfindet), ergibt sich ein sehr hoher Schutzbedarf nicht nur aus ausdrücklichen spezialgesetzlichen Regelungen, sondern auch deshalb, weil es sich um besondere Personendaten i. S. v. § 3 Abs. 4 Bst. a IDG handelt. Diese Haltung stimmt mit derjenigen der Bundeskanzlei überein, die gegenüber der Landeskanzlei ebenfalls festhielt, dass zur Wahrung des Stimmgeheimnisses bei jeder Wahl oder Abstimmung ein zusätzliches Couvert durch die Behörden beigelegt werden müsse.

2.2 ANSPRUCH AUF ÜBERSICHT ÜBER GESCHÄFTE DES GEMEINDERATES

Die ASD wurde von einer Privatperson angefragt, ob sie nach dem Öffentlichkeitsprinzip einen Anspruch auf Einsicht einer Pendenzenliste über Geschäfte des Gemeinderates habe.

Unter dem Öffentlichkeitsprinzip gemäss § 23 Abs. 1 IDG besteht grundsätzlich ein Anspruch, vom Gemeinderat die Pendenzenliste zu seinen Geschäften für einen bestimmten Zeitraum herauszuverlangen. Das Gesuch muss zwar nicht begründet werden, der Anspruch gilt jedoch nicht vorbehaltlos. Im Einzelfall kann das zuständige öffentliche Organ die Gewährung des Zugangs zu den verlangten Informationen aufgrund überwiegender öffentlicher oder privater Interessen verweigern oder einschränken. Bei einzelnen Geschäften könnte sich der Gemeinderat z. B. auf den Standpunkt stellen, dass seine freie Entscheidungsfindung gefährdet würde. In einem solchen Fall müsste das Gesuch nicht zwingend in Gänze abgewiesen werden, sondern es sollte ausreichen, Teile der Pendenzenliste zu schwärzen.

2.3 AUFZEICHNUNGEN BEI INTERNEN VIDEOKONFERENZEN

Die ASD wurde um Beratung eines kantonalen öffentlichen Organs gebeten, ob Aufzeichnungen bei internen Videokonferenzen zulässig und wenn ja, welche Vorkehrungen zur Einhaltung des Datenschutzes zu treffen seien.

Aus Sicht der ASD ist nicht ausgeschlossen, dass eine Aufzeichnung bei Videokonferenzen innerhalb der öffentlichen Verwaltung zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein kann, beispielsweise wenn alle, auch die aufgrund eines Schichtdienstes abwesenden Mitarbeitenden, Zugang zu ausgetauschten Informationen haben sollen. Dabei ist aber auf das Verhältnis zwischen Erfüllung der gesetzlichen Aufgabenwahrnehmung und der grundrechtlichen Beeinträchtigung zu achten. Es muss geklärt sein, ob die Aufzeichnung nur Äusserungen der Gesprächsteilnehmenden enthält oder ob auch Personendaten Dritter besprochen und damit bearbeitet werden und ob sich dies praktisch voneinander trennen lässt. Schliesslich kann nicht verkannt werden, dass Videoaufzeichnungen die möglichst freie Meinungsfindung und die Meinungsäusserung am Arbeitsplatz beeinträchtigen können und sich Mitarbeitende gehemmter und nicht gleich frei äussern wie ohne Aufzeichnung. Dem kann entgegengewirkt werden, indem die Aufnahmen nach einem kurzen Zeitraum vernichtet und nicht archiviert werden. Der Inhalt der Äusserungen darf

zudem nur einem rein fachlichen Austausch dienen. Es ist hilfreich, die datenschutzrechtlichen Vorgaben durch ein internes Nutzungsreglement klar zu umschreiben. In diesem Reglement sollte ebenfalls festgehalten sein, dass die temporäre Aufschaltung der Aufzeichnungen nicht automatisch erfolgt, sondern vorab geprüft wird und zu diesem Zeitpunkt Gesprächsteilnehmende bei Bedarf ein begründetes Veto gegen die temporäre Abrufbarkeit der Videokonferenz einlegen können. Die Aufzeichnungen müssen schliesslich i. S. v. § 8 IDG angemessen geschützt und nach der angegebenen kurzen Frist vernichtet werden.

2.4 HERAUSGABE VON TELEFONLISTEN AN ERZIEHUNGSBERECHTIGTE IN SCHULEN

Die ASD wurde durch die Leitung einer Schule angefragt, ob in Schulklassen Telefonlisten der Schüler und Schülerinnen an die Erziehungsberechtigten herausgegeben werden dürften.

Grundsätzlich sind aus Sicht der ASD Telefonlisten zur Weitergabe an Erziehungsberechtigte zum schnellen Informationsaustausch im Klassenverband ausserhalb der Schule erlaubt. Allerdings sind die Listen auf dafür tatsächlich benötigte Daten im Sinne des Grundsatzes der Verhältnismässigkeit zu beschränken. Dazu genügen Name, Vorname(n) und Telefonnummer des Schulkindes bzw. altersabhängig der Eltern. Die Wohnadresse wird zu diesem Zweck nicht benötigt. Allenfalls können die Adressen mit Einwilligung der Erziehungsberechtigten freiwillig zur Verfügung gestellt werden.

2.5 FRAGEN ZUR GEWÄHRUNG DES ZUGANGS ZU DEN EIGENEN PERSONENDATEN BEI GEMISCHTEN DOSSIERS/VORMUNDSCHAFTLICHEN AKTEN DER KESB

Eine KESB wandte sich im Rahmen eines eingegangenen Zugangsgesuchs an die ASD. Dabei wollte eine Person Einsicht in ca. 20 Jahre alte eigene Vormundschaftsakten. Aufgrund der darin enthaltenen sensitiven Informationen über die Eltern der gesuchstellenden Person wollte die KESB wissen, unter welchen Voraussetzungen und mit welchen allfälligen Einschränkungen die Einsicht zu gewähren sei.

Die Anfrage stützte sich auf das allgemeine Recht gemäss § 24 IDG, von einem öffentlichen Organ zu erfahren, ob es Daten über die eigene Person bearbeitet, und gegebenenfalls Zugang zu diesen erhalten. § 27 IDG statuiert mögliche Gründe, aufgrund derer das öffentliche Organ die Akteneinsicht einschränken könnte: Dabei handelt es sich insbesondere um entgegenstehende öffentliche Interessen oder private Interessen Dritter. Gerade bei Kindes- und Erwachsenenschutzakten, früher Vormundschaftsakten, handelt es sich oftmals um sogenannte «gemischte» Akten, d.h., dass sich in den Akten über die eigene Person auch Informationen über andere Personen finden. Einsicht kann dann gewährt werden, wenn die ausdrückliche Einwilligung der betroffenen Dritten vorliegt. Ist diese nicht gegeben, hat die entscheidungsbefugte Behörde allen Beteiligten eine Gelegenheit zur Stellungnahme zu gewähren und die daraus resultierenden Argumente abzuwägen. Überwiegt das Geheimhaltungsinteresse der Drittpersonen bzw. anderer öffentlicher Organe, sind deren Informationen nach § 28 IDG zu anonymisieren, wodurch die Einsicht eingeschränkt wird. Allerdings ist eine Anonymisierung gerade bei Akten des Kindes- und Erwachsenenschutzrechts schwierig, da die Identitäten der involvierten Personen der Gesuchstellerin oder dem Gesuchsteller bekannt sind.

Im konkreten Fall war die KESB in der glücklichen Lage, dass sie über eine gültige Einwilligung der betroffenen Drittpersonen verfügte. Ansonsten hätte eine Interessenabwägung durchaus schwierige Fragen aufwerfen können. Oftmals enthalten derartige Akten intime Informationen über Drittpersonen; andererseits gibt es für die Gesuchsteller neben den rein datenschutzrechtlichen Gründen, Einsicht in die Akten zu verlangen, weitere berechtigte Interessen. Die Akteneinsicht kann etwa einen wichtigen Beitrag leisten zur Aufarbeitung von traumatischen, in der Kindheit gemachten Erfahrungen.

2.6 ARBEITEN IM HOMEOFFICE

Aufgrund der Coronamassnahmen war eine Arbeit am Arbeitsplatz zeitweise nur in begründeten Ausnahmefällen möglich. Das Homeoffice wurde für viele Arbeitnehmende zum Alltag.

Die ASD wurde von verschiedenen Behörden anfragt, was in diesem Kontext aus Sicht des Datenschutzes besonders zu beachten sei. Im Homeoffice wie auch bei der Arbeit unterwegs unterstehen die Arbeitnehmenden denselben

rechtlichen Bestimmungen wie am ordentlichen betrieblichen Arbeitsplatz. Insbesondere müssen sie gewährleisten, dass auch im Homeoffice das Amtsgeheimnis sowie die datenschutzrechtlichen Bestimmungen jederzeit eingehalten werden. Auch hier gilt, dass organisatorische und technische Massnahmen zum Schutz der bearbeiteten Personendaten dem Risiko angemessen sein müssen: Je vertraulicher die Daten, desto stärker sind sie zu schützen. Zu den streng vertraulichen Personendaten zählen besondere Personendaten, bei deren Bearbeitung eine erhöhte Gefahr der Grundrechtsverletzung besteht (vgl. § 3 Abs. 4 IDG). Ebenfalls als streng vertraulich gelten Daten, die speziellen gesetzlichen Geheimhaltungspflichten unterstehen (Sozialversicherungsgeheimnis, Sozialhilfegeheimnis, Steuergeheimnis, Opferhilfe, Stimmgeheimnis).

Im Homeoffice gilt es dabei zwischen physischen und digitalen Akten zu unterscheiden:

An den Transport und die Aufbewahrung von physischen Unterlagen, die solche streng vertraulichen Personendaten enthalten, sind hohe Anforderungen zu stellen. Das heisst konkret, dass beim Transport abschliessbare Aktenkoffer erforderlich sind und die Aufbewahrung im Homeoffice abschliessbare Aktenschränke bedingt. Aufgrund der schwierigen Durchsetzbarkeit und Kontrollierbarkeit dieser Sicherheitsmassnahmen empfahl die Aufsichtsstelle Datenschutz, auf die Mitnahme und physische Bearbeitung solcher sensitiver Papierakten im Homeoffice wenn möglich zu verzichten. Hinzu kommt, dass Aktenkoffer beim Transport (z. B. im Zug) liegengelassen werden könnten und selbst diese Massnahme letztlich keinen hinreichenden Schutz bietet.

Bei der digitalen Arbeit ausserhalb des geschützten Netzwerks sollte der Zugriff auf Mailinfrastruktur, Dateiablage und Fachanwendungen nur via eine Remote-Access- bzw. VPN-Lösung mit Zwei-Faktor-Authentisierung erfolgen.

Aufgrund der Erfahrungen während der Pandemie und angesichts des geplanten Ausbaus der Möglichkeit zur Arbeit im Homeoffice hat die ASD der kantonalen Verwaltung Empfehlungen zu organisatorischen und technischen Massnahmen abgegeben, welche in die Telearbeitsrichtlinie und die Benutzerrichtlinie Informatikmittel einfliessen sollen.

2.7 STREAMING ODER VIDEOAUFNAHME DES WEIHNACHTSSPIELS IN DER SCHULE

Eine Schule suchte nach Alternativen, um ihr Weihnachtsspiel trotz der coronabedingten Einschränkungen durchführen zu können. Dabei standen die Videoaufnahme oder ein Streaming zur Diskussion. Die Schule gelangte an die ASD, um abzuklären, ob dies rechtlich möglich sei und welches die Voraussetzungen dafür wären.

Die ASD erklärte der Schule, dass es sich sowohl bei einem Streaming als auch einer Videoaufzeichnung um Datenbearbeitung handelt. Eine Notwendigkeit für die Durchführung des Schulauftrags war nicht gegeben, sodass die Videoaufnahme bzw. das Streaming nur gestützt auf eine rechtsgültige Einwilligung der Teilnehmenden möglich waren. Es gilt in solchen Fällen zu beachten, dass die von der Videokamera erfassten Personen über die Aufnahme, deren Art, Aufbewahrung und die Zugriffsrechte auf die Aufnahmen aufgeklärt werden. Die Einwilligung muss freiwillig und ohne Druck erfolgen, eine Ablehnung oder ein Rückzug muss jederzeit möglich sein und darf für die Betroffenen keine negativen Folgen haben.

Diese allgemeingültigen Rahmenbedingungen für eine Einwilligung – «Informed Consent» – stossen manchmal an gewisse Grenzen. So kann beispielsweise die Einwilligung nach erfolgtem Streaming de facto nicht mehr widerrufen werden. Aber auch nach einer Publikation im Internet ist es oft nicht möglich, die Einwilligung wirksam zu widerrufen. Selbst wenn der Inhalt vom Netz entfernt wurde, ist er über Archivseiten noch lange abrufbar. Deshalb steht die ASD auch einer uneingeschränkten Publikation im Internet selbst bei vorhandener Einwilligung eher kritisch gegenüber. In Fällen wie dem vorliegenden wäre es sicherer, Aufnahmen in einem passwortgeschützten Bereich einer «Closed User Group» zur Verfügung zu stellen.

2.8 ÜBERPRÜFUNG DER VORAUSSETZUNGEN ZUR RÜCKZAHLUNG VON SOZIALHILFEBEITRÄGEN

Eine Gemeindeverwaltung fragte bei der ASD nach, ob es zulässig sei, die Erfüllung der Voraussetzungen zur Rückzahlungspflicht von Sozialhilfebeiträgen durch einen Dritten prüfen zu lassen.

Die ASD erklärte, dass das Bearbeiten von Informationen, wozu auch die Abklärung einer Rückforderung von Sozialhilfebeiträgen gehört, Dritten übertragen werden kann, sofern keine rechtlichen Bestimmungen entgegenstehen. Es gilt dabei sicherzustellen, dass die Informationen nur so bearbeitet werden, wie es auch das öffentliche Organ dürfte. Weiter ist zu beachten, dass das öffentliche Organ die Verantwortung für den Umgang mit den Informationen behält, auch wenn diese durch Dritte bearbeitet werden. Diese Verantwortung erstreckt sich nicht nur auf Aspekte der Informationssicherheit, sondern ganz allgemein auf jede Datenbearbeitung. Aus diesem Grund ist es wichtig, dass bei der Ausarbeitung des Vertrages auf alle datenschutzrechtlichen Aspekte geachtet wird. Da der Auftragsdatenbearbeiter selbst in der Regel nicht dem IDG, sondern einem anderen Datenschutzgesetz untersteht (in der Schweiz dem Bundesgesetz über den Datenschutz DSG, in der EU i. d. R. der Datenschutz-Grundverordnung DSGVO), muss in den Verträgen gewissermassen Übersetzungsarbeit geleistet werden. Dabei werden die Grenzen, die das öffentliche Organ bei der Bearbeitung zu beachten hat, der Auftragsdatenbearbeiterin überbunden.

2.9 ERHEBUNG VON MAILADRESSEN ZUR VERSENDUNG VON RECHNUNGEN

Eine Gemeindeverwaltung wollte von der ASD wissen, ob sie die Mailadressen von Einwohnern auf freiwilliger Basis erheben dürfe, um auf diesem Weg Rechnungen zuzustellen.

Die ASD erläuterte, dass es keine Pflicht zur Angabe einer E-Mail-Adresse gibt, sie aber auf freiwilliger Basis erhoben werden kann. Dabei muss die Gemeindeverwaltung die Fälle, in welchen die Mailadresse verwendet wird, abschliessend nennen, denn wenn eine Person diese Daten freiwillig angibt, bedeutet dies nicht, dass fortan alle Kommunikation per E-Mail erfolgen kann. Über diesen Umstand muss die betroffene Person im Rahmen der Einwilligungseinholung informiert werden (Informed Consent). Aus Gründen der Informationssicherheit darf die meist unsichere E-Mail-Kommunikation nur eingeschränkt verwendet werden. Handelt es sich um Personendaten, deren Bearbeitung keine besondere Gefahr der Grundrechtsverletzung darstellt, können Rechnungen auf elektronischem Weg zugestellt werden. Auf keinen Fall darf die Mailadresse für den Versand von besonderen Personendaten und Daten, die einem speziellen Geheimnis (wie etwa dem Steuergeheimnis) unterliegen, verwendet werden.

2.10 BEKANNTMACHUNG DER DIAGNOSE ALS BEDINGUNG FÜR EINEN NACHTEILSAUSGLEICH

Eine Schulleitung machte für die Gewährung eines Nachteilsausgleichs zur Bedingung, dass die zugrundeliegende medizinische Diagnose der Schüler allen Lehrerpersonen, Schülern und deren Eltern bekanntgegeben wird.

Für die Bekanntgabe von besonderen Personendaten wie etwa einer medizinischen/psychiatrischen Diagnose bedarf es entweder der ausdrücklichen Verpflichtung bzw. Ermächtigung durch eine gesetzliche Grundlage oder der Erforderlichkeit zur Erfüllung einer in einem Gesetz ausdrücklich umschriebenen Aufgabe.

Das Bildungsgesetz sieht vor, dass die Schulleitung Massnahmen zur Umsetzung des Nachteilsausgleichs festlegt. Der Anspruch auf einen Nachteilsausgleich selbst wird jedoch durch eine Fachstelle festgestellt. Somit kommt die Verknüpfung der Massnahmenfestlegung mit der Bekanntmachung der Diagnose durch die Schulleitung einer faktischen Verweigerung des durch die Fachstelle bewilligten Nachteilsausgleichs gleich. Die Bekanntgabe an einen so weit gefassten Kreis ist nicht erforderlich zur Erfüllung des Bildungsauftrags der Schule. Dies bedeutet jedoch nicht, dass eine Bekanntgabe gewisser medizinischer Daten, insbesondere an Lehrpersonen, grundsätzlich ausgeschlossen wäre. Nur schon die Sicherheit des betroffenen Schülers oder der betroffenen Schülerin kann es notwendig machen, die Betreuungspersonen über eine medizinische Gefährdung zu informieren. Zu denken ist hier z. B. an Allergien, Diabetes, etc.

Eine solche Konstellation lag hier aber nicht vor, weswegen die ASD empfahl, auf die Bekanntgabe zu verzichten.

2.11 ADRESSAUSKUNFT AN ANWALTSKANZLEI IN DEN USA

Bei einer Gemeinde ging eine Adressanfrage einer Anwaltskanzlei aus den USA ein, da ein Investor aus der Schweiz möglicherweise von einem Anlagebetrug betroffen war. Zur Information und zur umfassenden Begleitung bat die Kanzlei um die gegenwärtige Adresse der umgezogenen Person.

Die ASD erklärte der Gemeinde, dass die Datenherausgabe von einzelnen Adressdaten an Private grundsätzlich gesetzlich zulässig ist, sofern keine Datensperre vorliegt. Bei Anfragen von Privatpersonen aus dem Ausland ist eine Datenherausgabe indes nur gestattet, sofern der Staat, in dem die Empfängerin registriert ist, über ein angemessenes Datenschutzniveau verfügt. Da dies für die USA gemäss Liste des Eidgenössischen Datenschutzbeauftragten nicht der Fall ist, ist eine Übermittlung der Adressdaten in die USA nicht zulässig. Die ASD riet der Gemeinde, den Investor über das Schreiben zu informieren. Dieser könne dann, sofern er dies wolle, direkt mit der Kanzlei Kontakt aufnehmen.

2.12 UMGANG DES KANTONS BASEL-LANDSCHAFT MIT COVID-ZERTIFIKATEN AM ARBEITSPLATZ

Die kantonale Covid-19-Verordnung wurde teilweise im Zweiwochentakt den neuen Verhältnissen angepasst. Vorliegende Auskunft ist daher eine exemplarische Momentaufnahme davon, wie der Arbeitgeber Kanton Basel-Landschaft zum Zeitpunkt der Anfrage mit Covid-Zertifikaten umgehen durfte.

Anlässlich der neugeschaffenen Möglichkeit der Verwendung eines Covid-Zertifikats gelangte das kantonale Personalamt an die Aufsichtsstelle Datenschutz. Es bat um eine datenschutzrechtliche Einschätzung, ob Lockerungen des Sicherheitskonzepts am Arbeitspatz möglich seien, wenn die Arbeitnehmenden Covid-Zertifikate nachweisen könnten. Insbesondere stellte sich die Frage, ob allenfalls eine Anpassung des Schutzkonzepts hinsichtlich einer Aufhebung der Maskenpflicht bei damit einhergehender Zertifikatskontrolle infrage komme und was dabei aus datenschutzrechtlicher Sicht zu beachten sei.

Die entsprechende Bestimmung der Covid-Verordnung führt aus, dass Arbeitgeber berechtigt waren, das Vorliegen eines Zertifikats zu überprüfen, wenn dies der Festlegung angemessener Schutzmassnahmen oder der Umsetzung des Testkonzeptes diente. Weitere Zwecke der Zertifikatserhebung waren unzulässig.

Die ASD qualifizierte vorab Covid-19-Zertifikate als besondere Personendaten, da in diesem Zusammenhang eine erhöhte Gefahr von Diskriminierung bestand. Entsprechend hohe Anforderungen für eine allfällige Datenbearbeitung wurden an eine gesetzliche Grundlage gestellt. In § 28 Personalgesetz erkannte die ASD eine genügende gesetzliche Regelung für eine Datenbearbeitung im Zusammenhang mit den Zertifikaten durch die dem Gesetz unterstellten Arbeitgeber. Die ASD wies darauf hin, dass eine allfällige Bearbeitung der Daten bzw. das Auslesen und Speichern der Zertifikatsinformationen möglichst datensparsam erfolgen müsse. So sollte der Kanton, sofern die Unterscheidung zwischen Immunitätsstatus (geimpft oder genesen) und Infektionsstatus (negativ oder positiv) für die Erstellung des Konzepts nicht notwendig war, nur das «Zertifikat Light» prüfen. Auch durfte die Kontrolle nicht flächendeckend stattfinden, sondern nur für Mitarbeitende in Arbeitssituationen, in welchen die Abstandsregelungen nicht eingehalten werden konnten. Bei Mitarbeitenden im Freien oder im Homeoffice etwa war eine Zertifikatskontrolle (zum Zwecke der Festlegung eines Sicherheitskonzepts ohne Maskenpflicht) nicht notwendig und daher nicht zulässig.

Abschliessend betonte die ASD die Notwendigkeit einer diskriminierungsfreien Regelung. Indes wäre eine solche schwierig umzusetzen gewesen, wenn Personen mit Zertifikat ohne Maske hätten arbeiten dürfen, Personen ohne Zertifikat indes eine Maske hätten tragen müssen. Faktisch hätte dies eine Datenbekanntgabe über den Impfstatus am Arbeitsplatz bedeutet: Personen mit einer Maske wären (in aller Regel) als Ungeimpfte identifiziert worden, da wohl nur sehr wenige geimpfte Personen ihr Zertifikat nicht vorgewiesen hätten, wenn sie dadurch von Erleichterungen hätten profitieren können.

In der Folge verzichtete der Kanton Basel-Landschaft für Verwaltungsmitarbeitende auf eine Kontrolle der Zertifikate und hielt an den bewährten bisherigen Schutzkonzepten fest. Erleichterungen für Arbeitnehmende mit Zertifikaten wurden nicht eingeführt.

Dieser Fall war in gewisser Hinsicht exemplarisch für die Corona-Zeit: Eine (bundes)rechtliche Massnahme implizierte eine Datenbearbeitung. Die Regelung des damit verbundenen Datenflusses erfolgte aber nicht überall in ausreichend klarer Weise. In der Folge kam es zu Unklarheiten in der Umsetzung. Die Datenbearbeitung in solchen Fällen betraf regelmässig eine hohe Anzahl von Personen, von denen ein erheblicher Anteil bereits der zugrunde liegenden Massnahme grundsätzlich kritisch gegenüberstand. Dadurch übertrug sich die intensive gesellschaftliche Diskussion über die Corona-Massnahmen in gewissen Fällen auf das Gebiet des Datenschutzes.

2.13 LISTENAUSKUNFT ZWECKS BESCHENKUNG ÄLTERER PERSONEN DURCH SCHÜLER

Schulklassen einer Gemeinde bastelten Windlichter, um Personen im Alter über 70 Jahren in der Weihnachtszeit damit zu beschenken. Die Gemeinde gelangte an die ASD mit der Anfrage, ob sie den Projektverantwortlichen die Adressdaten der betroffenen Personengruppe aushändigen dürfe und wenn ja, unter welchen Voraussetzungen.

Da jede Datenbearbeitung durch ein öffentliches Organ – unter dessen Begriff auch die Schule fällt – einer gesetzlichen Grundlage bedarf, prüfte die ASD vorab, ob aus einem Gesetz eine Aufgabe ersichtlich wäre, welche mit der «Aktion Windlicht» hätte erfüllt werden können. Die Identifikation einer solchen Aufgabe hätte die geplante Datenweitergabe als zulässig qualifiziert.

Letztlich qualifizierte die ASD eine allgemeine Norm aus dem Bildungsgesetz als genügende gesetzliche Grundlage. § 4 des Bildungsgesetzes statuiert den Bildungsanspruch eines Kindes bis zum Abschluss der Sekundarstufe II. Da sich das Bildungswesen gemäss § 2 Bildungsgesetz der christlichen, humanistischen und demokratischen Tradition verpflichtet sieht, befand die ASD, dass es mit dem Bildungsauftrag der Schule vereinbar ist, im Rahmen der christlichen Tradition zur Weihnachtszeit Geschenke für ältere Personen herzustellen. Eine Datenweitergabe der Einwohnergemeinde an die Schule befand die ASD daher als zulässig. Ausgenommen von der Möglichkeit der Adressweitergabe wurden indes durch Einwohnerinnen aktiv gesperrte Adressdaten.

Die ASD riet der Gemeinde, die Datenherausgabe an das vorhandene Verteilungskonzept zu knüpfen. Darin wurden zwei Lehrpersonen ernannt, die jeder Schülergruppe eine Liste mit den je benötigen Adressen für die Verteilung der Geschenke abgaben. Im Anschluss wurden die Listen durch die Lehrpersonen vernichtet.

3

VORABKONTROLLE

Die Vorabkontrolle wurde 2008 als präventives Instrument des Datenschutzes gesetzlich verankert. Im Rahmen dieses Prozesses 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. Dadurch können entsprechende Risiken bereits in einer frühen Phase des Projektes eingeschätzt und mit geeigneten Massnahmen reduziert werden. Dieses Vorgehen leistet einen wesentlichen Beitrag zur Etablierung wichtiger Prinzipien wie «Privacy by Design» und «Privacy by Default». 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.

Die der ASD zur Vorabkontrolle vorgelegten Projekte unterscheiden sich bezüglich Tragweite, Komplexität, eingesetzter Technologie und damit verbundenen Risiken stark voneinander. Die Aufsichtsstelle prüft nicht alle ihr vorgelegten Projekte, sondern die Selektion erfolgt risikobasiert. Die ASD hält die Durchlaufzeiten durchwegs so kurz wie möglich. Sie empfiehlt den verantwortlichen öffentlichen Organen gerade bei grösseren Projekten eine möglichst frühe Kontaktaufnahme und bietet die iterative Durchführung des Prüfprozesses in mehreren und dafür kleineren Einzelschritten an. Komplexe Projekte und vor allem Projekte mit Rechtsetzungsbedarf erstrecken sich teilweise über mehrere Jahre. Entsprechend kann sich der Zeitraum für die iterative Vorabkontrolle der einzelnen Projektdokumente ausdehnen.

Im Idealfall sind Sicherheitsbeauftragte und Rechtsdienste früh in Projekte eingebunden, sodass die Verantwortlichen des öffentlichen Organs, welches die Daten zur Aufgabenerfüllung bearbeitet, bei der notwendigen Analyse und Konzeption unterstützt werden. So verringert sich der Aufwand sowohl für das Projekt als auch die ASD deutlich. Die Erarbeitung von kantonalen Standards und Methoden, bei welcher die ASD mitwirken konnte, trägt zusammen mit der wachsenden Erfahrung ebenfalls dazu bei, dass der Aufwand pro Vorhaben für Behörden und ASD abnimmt.

Im Berichtsjahr sind 36 Projekte neu eingegangen, zu 13 davon hat die ASD auf Grund ihrer Risikobeurteilung keine Vorabkontrolle durchgeführt. Zwei Projekte aus zwei verschiedenen Direktionen wurden noch während der Vorabkontrolle in Betrieb genommen, also bevor die Stellungnahme der Aufsichtsstelle Datenschutz vorlag. Ein Projekt wurde zu spät im Projektablauf zur Vorabkontrolle vorgelegt.

Auch im Berichtsjahr fanden Arbeit und Schulunterricht mit digitalen Hilfsmitteln oft zu Hause statt, physische Treffen waren zeitweise nur sehr eingeschränkt möglich. Drei Vorabkontrollen befassten sich denn auch mit zentral betriebenen Kommunikationstechnologien. Die Häufung war auf die Corona-Massnahmen zurückzuführen, welche die Bedeutung des Arbeitens im Homeoffice und damit der digitalen Kommunikation verstärkten (bspw. für Softphone, Videoconferencing, Messenger-Dienst). Für die seit 2020 in Eile eingesetzten Lösungen musste im Berichtsjahr nachträglich eine solide Basis geschaffen werden, um sicherzustellen, dass die notwendigen technischen und organisatorischen Massnahmen zur Risikominimierung umgesetzt werden.

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 Kontrollen prüft die ASD die Umsetzung der rechtlichen, organisatorischen und technischen Vorgaben in öffentlichen Behörden in ihrem Zuständigkeitsbereich. Grundlage dafür bilden die eingereichten Unterlagen, Stichproben der erfolgten Bearbeitungsvorgänge, Interviews mit den Verantwortlichen sowie die vor Ort umgesetzten Massnahmen. Anders als bei der präventiven Vorabkontrolle in der Konzeptionsphase 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 Nachverfolgung der Umsetzung von Empfehlungen nach erfolgten Kontrollen. Die ASD geht davon aus, dass ihre Empfehlungen der Dringlichkeit entsprechend in angemessener Frist, in der Regel spätestens nach zwölf Monaten, umgesetzt werden. Ziel der Kontrollen ist nebst den konkreten Erkenntnissen zum Handlungsbedarf immer auch eine Sensibilisierung hinsichtlich effektiven Datenschutzes und der Angemessenheit der Informationssicherheitsmassnahmen. Um aus den Kontrollen Skaleneffekte zu erzielen, informiert der Datenschutzbeauftragte wenn möglich weitere Behörden mit gleichem Auftrag über Erkenntnisse aus Kontrollen.

4.1 CORONABEDINGT VERSCHOBENE PRÜFUNGEN

Aufgrund der auch im Berichtsjahr vom Bundesrat und Regierungsrat des Kantons Basel-Landschaft beschlossenen weiter andauernden Massnahmen gegen die Ausbreitung des Coronavirus entschied der Datenschutzbeauftragte, Prüfungen vor Ort auf die Zeit nach diesen Massnahmen zu verschieben. Vor diesem Hintergrund drängte es sich auf, eine Kontrolle mittels eines breitflächigen Self-Assessments bei öffentlichen Organen durchzuführen. Diese Methode wurde bei der Kontrolle der Betriebsordnungen zu den Videoüberwachungsanlagen in den Gemeinden angewandt.

4.2 KONTROLLE DER VIDEOÜBERWACHUNG IN DEN GEMEINDEN

Die Überwachung des öffentlichen Raums durch Polizei oder andere öffentliche Organe zum Zweck der Verhinderung oder Aufklärung von Straftaten hat in den letzten Jahren tendenziell zugenommen. Während die präventive Wirkung von Videoüberwachungsanlagen in der Wissenschaft umstritten ist, gibt es für die Aufklärung begangener Straftaten durchaus einen Nutzen. Die Überwachung des öffentlichen Raums stellt eine Bearbeitung von Personendaten dar und bedarf deswegen einer gesetzlichen Grundlage. Dabei hat die Rechtsprechung festgehalten, dass die Regelung der Videoüberwachung sich nicht in einer blossen Ermächtigung erschöpfen darf, sondern dass gewisse Rahmenbedingungen mitgeregelt werden müssen. Im Kanton Basel-Landschaft sieht die Regelung wie folgt aus: Die allgemeine gesetzliche Grundlage für Videoüberwachungen durch öffentliche Organe findet sich im Polizeigesetz, welches auch die Verhältnismässigkeit, die erlaubten Zwecke sowie die Aufbewahrung regelt. Zudem bestimmt das Gesetz, dass für jede Anlage ein Bearbeitungsreglement erlassen werden muss, und es gibt den minimalen Inhalt eines solchen Reglements vor. Damit soll sichergestellt werden, dass die Überwachungstätigkeiten nicht ausufern und jede Anlage rechtmässig betrieben wird. Die Verwendung des Begriffs «Betriebsreglement» im Polizeigesetz hat in der Vergangenheit bei den Gemeinden für Missverständnisse gesorgt, da ein Reglement auf Gemeindestufe ein Gesetz bezeichnet, das von der Gemeindeversammlung beschlossen werden muss. Dies war aber nicht die Absicht des Gesetzgebers, als er die Bestimmungen zur Videoüberwachung erliess, weswegen hier der Begriff «Betriebsordnung» verwendet wird.

Aus datenschutzrechtlicher Sicht vereint das Aufzeichnen von Personen mittels einer Videoanlage im öffentlichen Raum verschiedene Risiken für die Rechte und Freiheiten der Betroffenen. Eine erhebliche Anzahl von Personen ist in Alltagssituationen von der Datenbearbeitung direkt und unmittelbar betroffen. Deshalb hat die ASD die Überprüfung der Betriebsordnungen aller personenbezogenen Videoanlagen, welche von den Gemeinden betrieben werden, für eine Kontrolle ausgewählt. Ein Zweck der Kontrolle bestand auch darin, eine Einschätzung über den Gesamtbestand der Videoanlagen in den Gemeinden vorzunehmen. In der Folge wurden alle 86 Gemeinden schriftlich befragt.

Schwerpunkte der Kontrolle bildeten die Erhebung und Durchsicht der vorhandenen Betriebsordnungen zu personenbezogenen Videoanlagen, die Transparenz der Datenbearbeitung, die Aufbewahrungsdauer sowie die Zugriffsmöglichkeiten auf die Aufzeichnungen. Zudem wurden auch Augenscheine einzelner Anlagen genommen.

Zum Zeitpunkt der Kontrolle verfügten gemäss den per Selbstdeklaration erfolgten Rückmeldungen 26 der 86 Einwohnergemeinden über mindestens eine Videoüberwachungsanlage; insgesamt wurden 46 Anlagen gemeldet. Weder die Gemeindegrösse (bzw. die Anzahl Einwohner und Einwohnerinnen) noch die Lage innerhalb des Kantons erscheinen ausschlaggebend dafür, ob eine Überwachung erfolgt oder nicht. Auffällig war jedoch, dass die Anlagen in 3 Wellen errichtet wurden: Die meisten von ihnen wurden nämlich in den Jahren 2008/2009, 2014/15 und 2019/2020 in Betrieb genommen.

Überwacht werden oftmals öffentlich zugängliche Entsorgungssammelstellen der Gemeinden. Seltener überwacht werden Schul- und Sportplätze, Haltestellen des öffentlichen Verkehrs sowie die Gemeindeverwaltungen. Andere Orte mit Videoüberwachungsanlagen bestehen nur vereinzelt und scheinen aufgrund einer speziellen Gefährdungslage notwendig zu sein.

Es wurde festgestellt, dass die gesetzlichen Vorgaben betreffend den Erlass eines Betriebsreglements bei der Videoüberwachung von einem Grossteil der Gemeinden korrekt umsetzt wird. Nur vereinzelt wurde eine Verletzung der gesetzlichen Vorgaben festgestellt. Bestimmte gesetzliche Anforderungen bei der Datenbearbeitung wurden in einigen Fällen nicht erfüllt. Entsprechend bestand Handlungsbedarf, um ein angemessenes Niveau hinsichtlich Datenschutz und Informationssicherheit zu erreichen. Solchen Handlungsbedarf sah die Aufsichtsstelle Datenschutz namentlich in der inhaltlichen Ausgestaltung der Betriebsordnungen, insbesondere bei der Konkretisierung der Überwachung vor Ort. Zu bemängeln waren zudem die Zugriffsprozesse und die Klärung der Verantwortlichkeit, welche oftmals nur rudimentär beschrieben bzw. festgelegt wurden.

Im Schlussbericht wurden diese Erkenntnisse allen Gemeinden zur Kenntnis gebracht. Anders als in einem ordentlichen Kontrollschlussbericht wurden dabei nicht explizit die einzelnen Betriebsordnungen erwähnt, sondern das gewünschte, angemessene Datenschutzniveau beschrieben. Aufgabe der einzelnen Gemeinden ist es nun, ihre Videoüberwachungsanlagen mit den Vorgaben abzugleichen und entsprechende Verbesserungen selbstständig vorzunehmen.

4.3 KONTROLLE INFORMATIONSSICHERHEIT DER SCHULADMINISTRATIONSLÖSUNG SAL

Die basellandschaftliche Bildungs-, Kultur- und Sportdirektion (BKSD) betreibt zur Planung und Verwaltung des Schulbetriebes im Rahmen der kantonalen Vorgaben für die öffentlichen Schulen des Kantons Basel-Landschaft die Schuladministrationslösung SAL (vgl. § 59a–d Bildungsgesetz, SGS 640). Seit dem 1. Juli 2021 ist die Verordnung über den Betrieb der Schuladministrationslösung SAL (SGS 640.33) in Kraft, in der u. a. detaillierte Vorgaben bezüglich Zugriffsbeschränkung und -steuerung gemacht werden.

SAL wurde auf der Grundlage der Software „schulNetz" entwickelt und auf die Bedürfnisse der Schulen des Kantons Basel-Landschaft massgeschneidert. Alle Schulen der Sekundarstufe I, die Gymnasien und viele Primarschulen greifen auf das im Jahr 2015 eingeführte System zu. Hauptaufgabe von SAL ist die zentrale Verwaltung der Personendaten von Schülerinnen und Schülern, Erziehungsberechtigten, Lehrpersonen sowie von Personen mit einem pädagogisch-therapeutischen oder sonstigen schulbezogenen Auftrag.

Aus datenschutzrechtlicher Sicht vereint SAL verschiedene Risiken für die Rechte und Freiheiten der Betroffenen, v. a. besondere Personendaten, Datenbearbeitung durch mehrere öffentliche Organe, Zugriffe auf einen Datenbestand im sogenannten Abrufverfahren sowie involvierte Outsourcing-Partner.

Der Prüfumfang der Kontrolle umfasste folgende Bereiche: Informationssicherheits-Konzept «schulNetz» inkl. Risikomanagement, Sicherheit der Schnittstellen, Netzwerkinfrastruktur, Datensicherheit entlang des Datenlebenszyklus, Protokollierung und interne Kontrolle der Rechtmässigkeit der Datenbearbeitung.

Bei allen an der Prüfung Beteiligten war eine Sensibilisierung für die Themen Datenschutz und Informationssicherheit vorhanden. Bei der Prüfung stellte die ASD verschiedene organisatorische und technische Schwachstellen fest. In den organisatorischen Bereich fallen u. a. unzureichende Vereinbarungen mit Lieferantinnen und Dienstleistern. Empfehlungen sprach die ASD auch bezüglich Etablierung eines kontinuierlichen Informationssicherheits-Risikomanagements aus, um die Risiken und Massnahmen zur Reduzierung der Risiken effektiv zu steuern. Ausserdem wurde festgestellt, dass gewisse Massnahmen zum Schutz der Personendaten nicht angemessen waren. Die BKSD bestätigte der ASD, dass die Feststellungen korrekt sind und sie die entsprechenden Empfehlungen umsetzen wird.

5

ÖFFENTLICHKEITSPRINZIP

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

Direktion	Gesuche 2020	Gesuche 2021	gutgeheissen	teilweise gutgeheissen	abgewiesen
BKSD	2	0		0	0
BUD	1	1	1	0	0
FKD	1	1	0	1	0
SID	8	9	3	1	5
VGD	7	6	3	2	1
LKA	4	9	0	5	4
Total	**23**	**26**	**7**	**9**	**10**

Als das Öffentlichkeitsprinzip im Kanton Basel-Landschaft 2013 eingeführt wurde, bestand vereinzelt die Befürchtung, dass die Arbeit der öffentlichen Organe durch eine hohe Anzahl Gesuche eine spürbare Mehrbelastung erfahren könnte. Auch aus diesem Grund wurde eine Bestimmung in die Verordnung des IDG aufgenommen, wonach die Landeskanzlei auf kantonaler Ebene eine Erhebung der Gesuche nach § 23 IDG erstellt und der Aufsichtsstelle Datenschutz für ihre Berichterstattung weiterleitet. Diese Zahlen haben über die Jahre gezeigt, dass sich die Befürchtungen insgesamt nicht bewahrheitet haben. Auch dieses Jahr bewegen sie sich ungefähr im Rahmen des Vorjahrs, wie der oben aufgeführten Statistik zu entnehmen ist. Gegenüber dem Vorjahr ist eine Erhöhung der abgewiesenen bzw. nur teilweise gewährten Gesuche zu verzeichnen. Dies scheint auf eine Erhöhung von Gesuchen zurückzuführen sein, die entweder direkt Personendaten von Dritten betrafen oder in den Dokumenten Personendaten enthielten, die gemäss den gesetzlichen Bestimmungen anonymisiert werden mussten. Für die öffentlichen Organe ausserhalb der kantonalen Verwaltung liegen mangels Meldepflicht keine belastbaren Zahlen vor. Da die ASD im Berichtsjahr in ihrer Beratungstätigkeit aber keine grosse Veränderung in diesem Bereich feststellte, ist anzunehmen, dass auch in den Gemeinden sowie den anderen Behörden keine sprunghafte Veränderung stattfand. Wie auch in den Vorjahren standen in der Beratungstätigkeit zum Öffentlichkeitsprinzip insbesondere Verfahrensfragen im Vordergrund. Hier zeigt sich im Einklang mit den Erfahrungen anderer Kantone und denjenigen des Bundes, dass die Berücksichtigung und Abwägung der Interessen bei Vorliegen von privaten Interessen oftmals mehr Zeit benötigt, als es sich die Gesuchsteller wünschen.

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 Erarbeitung von Rahmenbedingungen und Anforderungen bei Beschaffungen bieten. Sie beriet die FIS ausserdem bei der Behandlung eines Ausnahmeantrags zu den Passwortrichtlinien und zeigte die damit verbundenen Risiken auf. Des Weiteren stellte die ASD der FIS die wichtigsten Änderungen vor, welche mit der Revision des IDG und der IDV auch auf die Sicherheitsbeauftragten zukommen.

6.3 DATENSCHUTZBEHÖRDEN ANDERER KANTONE

Die ASD arbeitete bei diversen Geschäften mit Datenschutzbehörden anderer Kantone zusammen, holte Einschätzungen zu Sachverhalten ein oder gab diese selbst ab. Gerade bei Datenbearbeitungen und Einschränkungen der Persönlichkeitsrechte aufgrund der Covid-Massnahmen bewährte sich auch im Berichtsjahr die in den vergangenen Jahren etablierte Zusammenarbeit und konnte weiter intensiviert werden. Die ASD unterstützte *privatim*, die Konferenz der schweizerischen Datenschutzbeauftragten, auch im Berichtsjahr, etwa bei der Beratung der Schweizerischen Informatikkonferenz (SIK) für neue Rahmenverträge mit Microsoft oder bei der Überarbeitung des Cloud-Merkblattes. Die ASD arbeitete auch eng mit diversen kantonalen Datenschutzbehörden zusammen für eine Stellungnahme zu Outsourcing-Verträgen im Zusammenhang mit einer gemeinsam genutzten e-Government-Plattform.

Im Rahmen dieser Zusammenarbeit mit anderen Aufsichtsbehörden kann sie ihr Fachwissen aufrechterhalten und vertiefen und ihre Haltung und Auslegung mit anderen Aufsichtsbehörden abgleichen. Zudem leistet sie einen Beitrag zur Verbesserung des Datenschutzes und der Informationssicherheit.

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 beratend und als IT-Revisorinnen und -Revisoren arbeiten. Der Schwerpunkt im Berichtsjahr lag beim Austausch über konkrete Projekte, kantonsübergreifend eingesetzte Lösungen und die Erarbeitung von Leitlinien beim Einsatz von MS-Clouddiensten.

6.5 AG SICHERHEIT

Die Arbeitsgruppe Sicherheit, welche von der ASD geleitet wird, traf sich im Berichtsjahr zweimal zum Austausch über datenschutzrechtliche Themen im Bereich der Sicherheit. Hier standen vor allem die Datenbearbeitungen durch die kantonalen Polizeikorps im Vordergrund. In diesem Bereich ist eine verstärkte Zusammenarbeit auf kantonaler Stufe zu verzeichnen. Viele Polizeikorps nutzen gleiche oder ähnliche technische Instrumente, so dass es sich anbietet, diese Themen auch von datenschutzrechtlicher Seite kantonsübergreifend zu betrachten.

Weitere Themen betrafen die Rechtsetzungsprojekte in einigen Kantonen, welche den (automatischen) Datenaustausch unter den Kantonen zum Thema haben. Hier stellt sich die Frage, auf welcher Ebene der Austausch am besten normiert werden kann.

Die Arbeitsgruppe Sicherheit wird punktuell von *privatim* mit der Ausarbeitung von Musterstellungnahmen im Rahmen von Bundesvernehmlassungen beauftragt. Solche Stellungnahmen ermöglichen es den Aufsichtsstellen, die im Kanton für die Vernehmlassung federführende Direktion auf datenschutzrelevante Aspekte aufmerksam zu machen; gleichzeitig bilden sie die Grundlage für eine (allfällige) eigene Stellungnahme von *privatim*.

6.6 AG GESUNDHEIT

Die Arbeitsgruppe Gesundheit hielt im Berichtsjahr fünf (Online-)Sitzungen ab. Aufgrund der Aktualität fand vorwiegend ein Austausch den datenschutzkonformen Umgang mit Corona betreffend statt. Obgleich die kantonalen Bestimmungen und Massnahmen sich teilweise erheblich unterschieden, war der Wissenstransfer äusserst hilfreich. Viele Fragestellungen konnten vertieft besprochen werden. Auch konnten viele übergreifende Probleme rechtzeitig erkannt und entsprechend vorgespurt werden. Trotzdem musste festgestellt werden, dass viele erprobte Prozesse und Abläufe in den Kantonen während der Pandemie nicht angewendet werden konnten. Bedingt durch das anfängliche Unwissen über die Gefährlichkeit von Covid-19 wurden viele rechtliche Regelungen in kürzester Zeit immer wieder überarbeitet und angepasst. Entsprechende Datenbearbeitungsvorgänge mussten rasch ermöglicht und später verbessert werden, was eine Kontrolle von und Beratung über die Sicherheit der Daten in den Kantonen erheblich erschwerte.

6.7 AG-DIGITALE VERWALTUNG

Die Arbeitsgruppe traf sich im Berichtsjahr einmal. Ein Schwerpunktthema war die Vereinbarkeit des «Once-Only-Prinzips» mit den geltenden gesetzlichen Rahmenbedingungen sowie Rahmenbedingungen, welche bei solchen Vorhaben aus Sicht des Datenschutzes berücksichtigt werden müssen. *privatim* hat dazu eine unabhängige Expertise in Auftrag geben.

6.8 KOORDINATIONSGRUPPE ZUM SCHENGENER INFORMATIONSSYSTEM (SIS)

Die Schweiz hat sich beim Beitritt zu Schengen unter anderem dazu verpflichtet, regelmässig die rechtmässige Anwendung der Informationssysteme durch die Behörden zu prüfen. Da diese Systeme vom Bund betrieben, aber auch von den Kantonen genutzt werden, müssen entsprechende Kontrollen zuständigkeitshalber sowohl von den kantonalen Aufsichtsstellen als auch vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) durchgeführt werden. Die Schengen-Koordinationsgruppe ist dabei ein gesetzlich vorgesehenes Gefäss zum Zwecke des Erfahrungs- und Wissensaustauschs sowie der Koordination dieser Kontrollen. Die Gruppe traf sich im vergangenen Jahr zweimal virtuell. Dabei wurde unter anderem beschlossen, den von der Gruppe 2019 ausgefertigten Leitfaden für die Kontrollen einer Überarbeitung zu unterziehen.

7

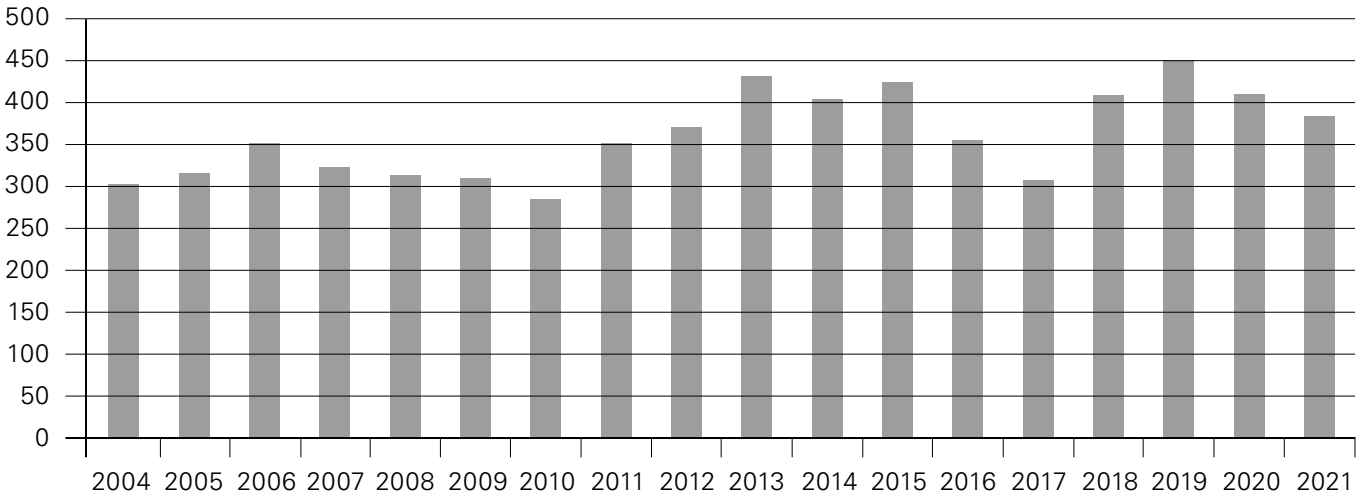
SCHULUNGEN UND REFERATE

Wie jedes Jahr führte die ASD auch 2021 wieder eine Reihe von Schulungen durch, auch wenn vereinzelte Veranstaltungen aufgrund der Pandemie bzw. wegen zu weniger Anmeldungen abgesagt werden mussten. Da die revidierten Bestimmungen des IDG erst seit 1. Januar 2022 gelten, erwartet die ASD jedoch für 2022 eine leichte Erhöhung, da verschiedene öffentliche Organe bereits Interesse angemeldet haben, sich über die Änderungen zu informieren. Bereits im Berichtsjahr konnte die Fachgruppe Informationssicherheit den zentralen und dezentralen Sicherheitsbeauftragten der kantonalen Verwaltung über die wichtigsten revidierten Bestimmungen informieren. Wie jedes Jahr führte die ASD auch 2021 den überbetrieblichen Kurs (üK) der Branche «Öffentliche Verwaltung» zum Thema «Datenschutz und Öffentlichkeitsprinzip» für die kantonalen Lernenden durch. Die jüngsten der kantonalen Mitarbeitenden zu informieren, ist der ASD sehr wichtig. Einerseits werden sie damit zu einem sehr frühen Zeitpunkt für die Verantwortung, die sie mit der Bearbeitung von Personendaten tragen, sensibilisiert, andererseits sind sie als vollkommene «Digital Natives» in der Regel von klein auf mit Kommunikationstechnologien vertraut. Damit fallen auch Informationen über die Informationssicherheit auf fruchtbaren Boden. Im Idealfall können die Kursbesucherinnen und Kursbesucher sogar den einen oder anderen Impuls für den persönlichen Umgang mit Kommunikationstechnologien mitnehmen.

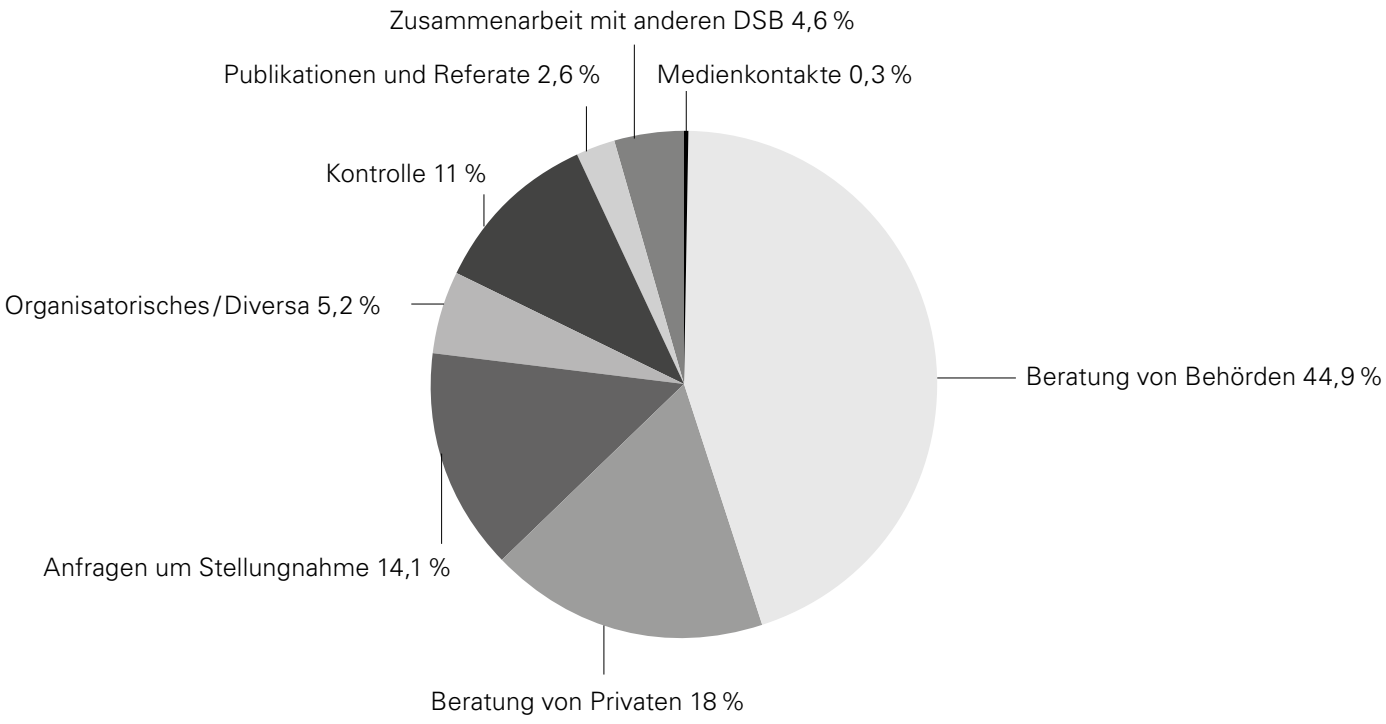
8

ANHANG

ANZAHL NEU ERÖFFNETE GESCHÄFTE



ART DER GESCHÄFTE



(Basis: Anzahl neu eröffnete Geschäfte, Prozentanteile gerundet)