BASEL LANDSCHAFT

TÄTIGKEITSBERICHT 2024 DER AUFSICHTSSTELLE DATENSCHUTZ

INHALTSVERZEICHNIS

1

DAS JAHR 2024

1.1 DIE AUFSICHTSSTELLE DATENSCHUTZ (ASD)

Die ASD ist eine unabhängige Aufsichtsbehörde. Sie verfügt über fundiertes Fachwissen bezüglich Datenschutz, Umgang mit Informationen, Informationssicherheit und die damit verbundene Governance. Als unabhängige Aufsichtsbehörde ist die ASD, wie auch die Ombudsstelle 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, Vorabkonsultationen, 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 378 Geschäftsdossiers eröffnet. Der Aufsichtsstelle werden zunehmend mehr neue Vorhaben zur Vorabkonsultation vorgelegt, im Berichtsjahr 74. Bei 20 Vorhaben entschied die ASD, keine Vorabkonsultation durchzuführen. Es wurden vier Datenschutzkontrollen abgeschlossen, 155 Beratungen bei öffentlichen Organen und 61 bei Privatpersonen durchgeführt sowie sieben Schulungen und Referate gehalten. Die ASD wurde für 21 Stellungnahmen angefragt und verfasste weitere 119 Stellungnahmen im Rahmen von Vorabkonsultationen. In 51 Geschäftsfällen hat die ASD mit Aufsichtsbehörden anderer Kantone zusammengearbeitet.

Auch in diesem Berichtsjahr war die ASD mit diversen komplexeren und umfassenderen Aufgabenstellungen konfrontiert.

Der ASD standen für diese Aufgaben 530 Stellenprozente zur Verfügung, welche sich auf sieben Personen verteilten. Ausserdem unterstützten Frau Gülcan Walther und Frau Celina Clavadetscher die ASD tatkräftig im Rahmen des jeweils sechsmonatigen Volontariates für Juristen und Juristinnen, welches die ASD auch im Berichtsjahr anbot.

1.2 KÜNSTLICHE INTELLIGENZ

Künstliche Intelligenz (KI) ist ein spannender Ansatz zur Lösung von Problemstellungen, die mit herkömmlichen Methoden schwer zu lösen sind oder die bislang gar nicht gelöst werden konnten. In einigen Bereichen gibt es vielversprechende Ansätze, die sich teilweise bereits etabliert haben – die Entwicklung ist rasant. Spätestens seit dem Start von ChatGPT für die breite Öffentlichkeit Ende 2022 ist das Thema omnipräsent – auch bei staatlichen Akteuren.

Künstliche Intelligenz (KI) ist aktuell ein Hype-Thema. Auch die ASD wird immer wieder mit Fragen zum Einsatz von KI konfrontiert. Dabei stellt sich zuerst – wie oft bei solchen Themen – das Problem, dass es keine eindeutige oder einheitliche Definition dessen gibt, was genau unter KI zu verstehen ist. Das überrascht kaum, da selbst der Begriff der Intelligenz bereits zu ausufernden Diskussionen führen kann. Dies noch, bevor überhaupt auf die Frage eingegangen wird, ob Intelligenz künstlich, in einem IT-System abgebildet oder nachempfunden sein kann. Zudem ist zu beobachten, dass von Anbietern Lösungen für alle möglichen Bereiche versprochen werden und der Eindruck entstehen kann, dass KI «die eine Lösung» für alles ist. Die tatsächliche Realisierbarkeit ist jedoch in vielen Bereichen (noch) nicht belegt. Zudem sind potenziell unerwünschte Effekte sowie Risiken bei vielen der möglichen Anwendungsfälle noch nicht ausreichend analysiert. Das ist allerdings kein KI-spezifisches Phänomen, sondern ein Effekt, der regelmässig im Zusammenhang mit dem Hype um «neue Technologien» zu beobachten ist.

Unbestritten handelt es sich bei KI-Ansätzen anders als bei herkömmlichen Algorithmen um eine Herangehensweise, bei der die Logik nicht durch klar definierte Abfolgen fest programmiert wird. Das Resultat einer Anfrage wird aufgrund von Trainings auf Daten bestimmt. Daraus ergibt sich, dass der Datenbasis und der Art des Trainings eine hohe Bedeutung zukommt. Die KI ist zum aktuellen Zeitpunkt grossmehrheitlich eine Blackbox, deren Resultate meist nur indirekt verifiziert und beurteilt werden können.

Die oft ins Feld geführte Annahme, dass vor allem die Quantität relevant sei und die Qualität der Daten dabei keine zentrale Rolle spiele, erscheint abwegig – darauf wird auch zunehmend in Fachartikeln hingewiesen. Unbestritten ist, dass sich die zugrunde liegende Logik nicht im klassischen Sinn nachvollziehen lässt und gewisse Aspekte, wie das sogenannte «Halluzinieren»[2], bislang nicht ausreichend erklärbar sind. Gerade wenn solche Algorithmen auf

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

[2] Antworten» einer KI, die erfunden oder irreführend sind. Diese können überzeugend und plausibel klingen.

Personen angewandt werden sollen, müssen diese Punkte genauso gebührend berücksichtigt werden wie der Umstand, dass eine KI letztlich «nur» eine auf Wahrscheinlichkeit beruhende Einteilung in «Schubladen» vornimmt. Zu beachten ist zudem, dass bei grossen Datenmengen oder komplexen KI-Modellen oft sehr schwierig abgeschätzt oder entschieden werden kann, ob eine beobachtete Korrelation tatsächlich kausaler Natur ist.
Unbestritten ist auch die hohe Rechenintensität, die benötigt wird und zum aktuellen Zeitpunkt meist nicht on-premise bereitgestellt werden kann. Mit dem in der Regel intern nicht vorhandenen oder noch nicht aufgebauten Fachwissen im Bereich von KI führt dies dazu, dass die meisten KI-Lösungen aktuell mit einer Auftragsdatenbearbeitung einhergehen. Wie bei jedem anderen Vorhaben auch müssen die Anforderungen an eine solche beachtet und erfüllt sein (vgl. Kap. 1.3 Auftragsdatenbearbeitung). Häufig erfolgt die Verarbeitung in einer Cloud – mit denselben Risiken, die auch andere «Software as a Service»-Lösungen[3] bergen. Unabhängig vom Betriebsmodell – also auch bei On-Premises-Lösungen – müssen die KI-spezifischen Fragen hinsichtlich der Gesetzeskonformität und der mit der Bearbeitung einhergehenden Risiken bei Projekten mit KI in der Anfangsphase beantwortet werden.
Für viele der bis anhin der ASD vorgelegten «einfachen» Anwendungsfälle sind aus Sicht der ASD die aktuell geltenden gesetzlichen Grundlagen ausreichend. Bei diesen Vorhaben sind oft die spezifischen KI-Risiken aus Sicht Datenschutz geringer als jene, die sich aus der Auftragsdatenbearbeitung in einer Cloud ergeben. Anwendungen, die Mitarbeitende ausschliesslich beim Korrigieren, Übersetzen, Erstellen oder Zusammenfassen von Texten unterstützen, bergen in der Regel primäre (Datenschutz-)Risiken, die sich aus der Übermittlung an die Auftragsdatenbearbeiterin und ihrer Bearbeitung ergeben und nicht aus dem Einsatz einer KI. Dennoch müssen die Fragen nach Zuverlässigkeit, Korrektheit und Verifizierbarkeit durch die Nutzerinnen und Nutzer selbstverständlich zwingend geklärt werden. Auch geht die ASD aktuell davon aus, dass bei solchen KI-Lösungen keine Personendaten für Trainingszwecke verwendet werden dürfen (§ 11 IDG, Zweckbindung sowie das Risiko, dass Personendaten in der Folge Dritten bekanntgegeben werden könnten).
Die ASD beobachtet die laufenden Entwicklungen und prüft derzeit eingereichte Vorhaben im Einzelfall. Positiv zu erwähnen gilt es an dieser Stelle auch, dass sich die Verwaltung des Kantons Basel-Landschaft dem Thema KI aktiv stellt, ohne aktuell in überstürzten Aktionismus zu verfallen. Abschliessend ist festzuhalten, dass es für die Exekutive, aber auch für die ASD in ihrer Aufsichtsfunktion mehr als nur wünschenswert ist, dass über die Nutzung von KI-Systemen sowohl gesellschaftliche als auch politische Debatten geführt werden und daraus resultierend möglichst klare Vorgaben entstehen. Entscheidungen in einem derart weitreichenden und einschneidenden Themenfeld können und dürfen weder alleine von der Exekutive noch von einer Aufsichtsbehörde getroffen werden. Die ASD ist ihrerseits bereit, sich in diesen Prozess sachlich, differenziert und konstruktiv mit ihrem Fachwissen einzubringen.

1.3 AUFTRAGSDATENBEARBEITUNG

Im Tätigkeitsbericht 2023 hatte die ASD ein paar allgemeine Ausführungen zu den datenschutzrechtlichen Rahmenbedingungen der Auftragsdatenbearbeitung im Sinne von § 7 IDG dargestellt. Dort wurde die Notwendigkeit für den Abschluss einer vertraglichen Regelung der Bearbeitung der Personendaten zwischen dem öffentlichen Organ und der Auftragsdatenbearbeiterin erläutert. Zur Erinnerung: Eine vertragliche Regelung ist unter anderem auch deshalb notwendig, weil die privaten Dienstleister nicht dem gleichen Datenschutzgesetz wie das öffentliche Organ unterstehen, weshalb die Pflichten, die sich für den Auftraggeber aus dem IDG ergeben, dem Vertragspartner überbunden werden müssen. Was aber genau muss vertraglich geregelt werden, und wo liegen in der Praxis die Stolpersteine?
Seit ein paar Jahren ist es bei Dienstleistern gängige Praxis, dass die Rechte und Pflichten betreffend die Bearbeitung von Personendaten in einem separaten Vertragsbestandteil, oft «Auftragsdatenbearbeitungsvereinbarung» (ADV) oder «Data Processing Agreement» (DPA) genannt, festgelegt werden. Bei Produkten «von der Stange» sind die Regelungen oftmals in den Allgemeinen Geschäftsbedingungen (AGB) der Anbieterin enthalten. Bisweilen wird im Vertragswerk auch auf die von der Digitalen Verwaltung Schweiz (DVS) herausgegebenen AGB für IKT-Dienstleistungen verwiesen, in denen ebenfalls datenschutzrelevante Punkte enthalten sind.
Die Bezeichnung oder die Herkunft des Vertrags spielt dabei letztlich nur eine untergeordnete Rolle, wichtig ist der Inhalt und Detaillierungsgrad der getroffenen Regelungen. Und hier gilt es aufzupassen. Gerade wenn die Vertragsentwürfe vom Anbieter stammen, sei es in der Form von massgeschneiderten Verträgen oder AGB, enthalten diese oftmals Klauseln, die einseitig zugunsten der Anbieterin formuliert sind und den speziellen Anforderungen, die sich aus der

[3] Anwendungen, die über das Internet zur Verfügung gestellt werden, Nutzer greifen i.d.R. über einen Webbrowser zu – Hardware, Software und Daten liegen exklusiv bei der Anbieterin.

rechtlichen Situation des öffentlichen Organs ergeben, nicht genügen. Folgend ein paar wichtige Aspekte – eine abschliessende Auflistung ist im Merkblatt «Auftragsdatenbearbeitung» zu finden.

Geregelt werden müssen der Umgang der Datenbearbeitung sowie der Zweck, zu welchem die Daten bearbeitet werden. Die Vertragspartnerin muss dabei insbesondere verpflichtet werden, die Personendaten nicht zu anderen, eigenen Zwecken zu verwenden. Die Auftragsdatenbearbeiterin hat sich sowie ihre Mitarbeitenden zur Vertraulichkeit zu verpflichten. Zudem darf sie die Datenbearbeitung ohne schriftliche Genehmigung des öffentlichen Organs nicht einem weiteren Dritten, einer Unterauftragsbearbeiterin übertragen (§ 7 Abs. 3 IDG). Alternativ zur schriftlichen Einwilligung kann mit der Auftragsdatenbearbeiterin eine Informationspflicht für Änderungen bezüglich der eingesetzten Subunternehmen vereinbart werden. In diesem Fall muss darauf geachtet werden, dass das öffentliche Organ – wenn es den neuen Subunternehmer nicht akzeptieren kann – das Auftragsverhältnis auflösen kann und muss. Die Wirkung, dass nach Vertragsabschluss die Auftragsdatenbearbeiterin nicht eigenständig nach Belieben Subunternehmer beiziehen kann, bleibt gleich. In beiden Fällen bleibt die Herausforderung für das öffentliche Organ, dass es ausserordentlich und innert kürzester Zeit einen Ersatz finden muss. Damit es dieser Pflicht Folge leisten kann, müssen die Verantwortlichen bereits vor Vertragsabschluss ein Exitszenario ausarbeiten, welches bei Vertragskündigung aktiviert werden kann. Die bereits bei Vertragsabschluss bestehenden Subunternehmen müssen genannt werden und gelten mit Vertragsunterzeichnung als akzeptiert.

Die Auftragnehmerin hat zudem über ihre zur Gewährleistung der Informationssicherheit getroffenen technischen und organisatorischen Massnahmen zu informieren, da das öffentliche Organ gegenüber den betroffenen Dritten auch dafür die Verantwortung trägt und demnach beurteilen muss, ob die Datenbearbeitung beim Vertragspartner sicher erfolgt. Weitere Punkte sind unter anderem die Regelung für den Fall, dass eine Anfrage zum Zugang zu den Daten bei der Auftragnehmerin eingeht, die Massnahmen bei einer Datenschutzverletzung sowie die Kontrollrechte des öffentlichen Organs bei der Auftragnehmerin.

Fast jeder Vertrag endet irgendwann, sodass auch die Modalitäten wie die Rückgabe der Daten oder die Vernichtung bei der Auftragsdatenbearbeiterin für diesen Fall geregelt werden müssen. Dieser Punkt ist auch deshalb entscheidend, weil ohne ein realistisches Exitszenario die Gefahr einer Abhängigkeit («locked-in») besteht.

Für die Durchsetzung vertraglicher Ansprüche sind das anwendbare Recht sowie der Gerichtsstand wichtig. Auch wenn die Festsetzung eines ausländischen Rechts und Gerichtsstands nicht per se ausgeschlossen ist, rät die ASD regelmässig zur Anwendbarkeit des Schweizer Rechts mit einem inländischen Gerichtsstand.

In der Praxis stellt die ASD fest, dass sich vor allem im Bereich der Zweckbindung, der Kontrollrechte, aber auch betreffend den Beizug von Unterauftragsdatenbearbeiterinnen viele Anbieter weitergehende Rechte einräumen lassen möchten oder weniger Pflichten zu übernehmen bereit sind. Heikel ist auch der oftmals anzutreffende Mechanismus, dass die Datenbearbeitungsmodalitäten einseitig durch den Anbieter abgeändert werden können. Dadurch besteht das Risiko, dass durch eine solche Änderung eine rechtmässige Auftragsdatenbearbeitung unrechtmässig wird. Hier muss zumindest eine Vorabinformationspflicht festgesetzt werden sowie das Recht, bei einer inakzeptablen Änderung den Vertrag kündigen zu können.

Gewisse der oben genannten Punkte mögen sogenannt «risikofähig» sein, das heisst, eine nicht optimale Regelung erhöht das Risiko einer Datenbearbeitung, ist aber nicht direkt rechtswidrig. Dieses Risiko muss korrekt ausgewiesen, das Schadensausmass beurteilt und vom öffentlichen Organ oder von dessen vorgesetzter Stelle getragen werden. Gewisse andere Punkte wie die Zweckbindung oder die Modalitäten bei Änderungen von Subunternehmen entziehen sich jedoch einer Risikobetrachtung, weil sie gesetzlicher Natur sind. Hier hat das öffentliche Organ keinen Spielraum.

Die ASD ist sich durchaus bewusst, dass die Gestaltung von guten Auftragsdatenbearbeitungsverträgen gerade auch für kleinere Behörden anspruchsvoll sein kann, da oft auch intern nicht immer das erforderliche rechtliche und technische Know-how zur Verfügung steht. Dennoch ist es eine Aufgabe, die das öffentliche Organ zu erfüllen hat, da es für die Datenbearbeitung des Auftragnehmers vollumfänglich verantwortlich bleibt. Als Hilfe stellt die ASD ihr Merkblatt über die Auftragsdatenbearbeitung zur Verfügung. Damit kann das öffentliche Organ anhand einer Checkliste den Entwurf des Vertragswerks auf die kritischen Aspekte überprüfen.

2

AUS DEM BERATUNGSALLTAG

2.1 VERSAND DER PATIENTENLISTE EINES SPITALS AN SEELSORGER

Eine Privatperson wandte sich an die ASD mit der Frage, ob es zulässig sei, dass ein Spital, das sich auf der kantonalen Spitalliste befindet, alle zwei Wochen eine Liste mit allen stationären reformierten Patienten an die evangelisch-reformierte Kirchgemeinde sende.

Auf Nachfrage der ASD führte das Spital aus, dass jeweils eine Patientenliste der im Zuständigkeitsbereich wohnenden Personen alle zwei Wochen direkt an die römisch-katholischen und evangelisch-reformierten Pfarrpersonen gesendet werde. Durch den direkten Versand sei auch das Seelsorgegeheimnis sichergestellt. Diagnosen oder medizinische Befunde würden nicht mitgeteilt. Mitgeteilt würden Name, Adressdaten, Geburtstagsdatum, Eintrittsdatum und Zimmernummer.

Rechtsgrundlage für die Weitergabe der Daten sei die Verordnung über die Spitalseelsorge der Landeskirchen. Diese verpflichte die kantonalen Spitäler, den von den Landeskirchen gewählten und angestellten Spitalseelsorgenden die für den seelsorgerlichen Dienst notwendigen Informationen zur Verfügung zu stellen. Den Seelsorgerinnen und Seelsorgern werde so die Betreuung Gemeindeglieder ermöglicht. Zudem würden nicht alle Patienten auf den entsprechenden Patientenlisten erscheinen, vielmehr würden nur jene Personen aufgeführt, welche seelsorgerische Betreuung wünschten und dies auf dem Anmeldeformular entsprechend vermerkten.

Die ASD stellte fest, dass die Bekanntgabe gestützt auf die Verordnung über die Spitalseelsorge der Landeskirchen erfolgt. Allerdings besteht die entsprechende Bestimmung im Spitalgesetz, die den Regierungsrat zum Erlass dieser Verordnung ermächtigte, seit Längerem nicht mehr. Das Spitalgesetz von 1976 war mehrfach geändert worden, es ist für die ASD nicht genau nachvollziehbar, wann und aus welchem Grund die Delegationsnorm gestrichen worden ist.

Die Frage nach dem rechtlichen Status der Verordnung kann jedoch offenbleiben, da das Spital immer auch eine Einwilligung der betroffenen Patienten zur Weitergabe der Informationen an die zuständige Pfarrperson einholt. Demnach erweist sich das Vorgehen des Spitals trotzdem als rechtmässig.

2.2 RÜCKFÜHRUNG VON PERSONENDATEN

Anlässlich eines konkreten Falles hatte die ASD zu beurteilen, ob eine Organisation, der die Erfüllung öffentlicher Aufgaben übertragen worden war, die von ihr bearbeiteten Dossiers nach Ablauf des Vertrags mit dem Gemeinwesen behalten darf oder sogar muss.

Eine Organisation gilt während der Zeit, in der sie öffentliche Aufgaben erfüllt, als öffentliches Organ im Sinne des IDG. Sie kann sich für die Bearbeitung der Personendaten auf das IDG sowie die entsprechende Sachgesetzgebung stützen. Nach Beendigung der Leistungsvereinbarung mit dem Gemeinwesen gilt die Organisation nicht mehr als öffentliches Organ, womit die Rechtsgrundlage für die Weiterbearbeitung der Daten entfällt. Da mit der Beendigung der Leistungsvereinbarung die öffentliche Aufgabe wieder auf das Gemeinwesen zurückfällt, muss jenes in die Lage versetzt werden, die offenen Fälle zu bearbeiten. Somit ist klar, dass die jeweilige Organisation diese Unterlagen herausgeben muss.

Was aber gilt für bereits abgeschlossene Fälle? Das Aufbewahren von Personendaten gilt gemäss § 3 Abs. 5 IDG ebenfalls als eine Form des Bearbeitens. Mit dem Wegfall der Leistungsvereinbarung entfällt somit auch die Rechtsgrundlage für die Aufbewahrung der bereits abgeschlossenen Fälle, auch diese müssen zurückgegeben werden.

Von wem die Daten ursprünglich erhoben worden sind, ist irrelevant. Die Datenbearbeitung ist geknüpft an die Erfüllung der öffentlichen Aufgabe, somit müssen sich die Daten beim aktuell zuständigen öffentlichen Organ befinden.

Dies schliesst jedoch nicht aus, dass eine vormals zuständige Organisation gewisse Informationen, die im Zusammenhang mit der Übertragung der öffentlichen Aufgabe stehen, behalten darf. Die jeweilige Organisation muss gegebenenfalls in der Lage sein, Rechenschaft über die Aufgabenerfüllung ablegen zu können, mindestens so lange, als vertragliche Ansprüche durch das Gemeinwesen geltend gemacht werden können. Diese Informationen schliessen jedoch die materiellen Dossiers nicht mit ein.

2.3 SPEICHERUNG VON LUFTAUFNAHMEN IN EINER CLOUD

Die ASD erhielt eine Anfrage von einer kantonalen Behörde zur Speicherung der Rohdaten von Luftaufnahmen und Umgebungsbildern, welche in Einzelfällen Personen enthalten. Zur Nachvollziehbarkeit von Aufträgen sollen die Luftaufnahmen bis zur Erreichung der gesetzlichen Löschfrist gespeichert werden. Die Behörde beabsichtigte, für das Speichern der sehr grossen Datenmengen eine kostengünstige Lösung einzusetzen. Da innerhalb des Kantons für diese Anforderungen keine Lösung zur Verfügung steht, wurden auch Cloud-Lösungen ausserhalb der Kantonsumgebung in Erwägung gezogen. Das Datenschutzrisiko bezüglich Datenbearbeitung von Personendaten in der Cloud sollte jedoch verringert werden.

An die ASD wurde die Frage gerichtet, ob die genannten Luftaufnahmen auch nach lokaler Verschlüsselung (Schlüssel lokal, sicheres und lokal durchgeführtes Verschlüsselungsverfahren) als Personendaten einzustufen sind.

Die ASD wies darauf hin, dass nach geltender Rechtslage (§ 11 Abs. 2 IDG) die Bilder, auf denen Personen erkennbar sind, schnellstmöglich anonymisiert werden müssen (bspw. mit Blurring verwischt), da die Bearbeitung der Personendaten für die Aufgabe der anfragenden Behörde nicht notwendig ist. Inwiefern die Qualität der Bilddaten durch das Blurring gemindert und die Aufgabe der Behörde dadurch erschwert wird, ist der ASD nicht bekannt.

Wenn die Rohdaten von der Behörde vor der Speicherung in der Cloud verschlüsselt werden, sind diese aus Sicht der Cloud-Anbieterin zwar «anonymisiert», der Behörde sind diese jedoch mittels Schlüssel zugänglich. Die ASD geht aufgrund der dargelegten Anwendungsfälle davon aus, dass die Aufbewahrung der Originalbilder dem Zweck der Einzelfall-bezogenen Qualitätskontrolle dient. Sobald diese Qualitätskontrolle erfolgt ist, müssen die Rohdaten gem. § 15a Abs. 4 der kantonalen Verordnung über Geoinformation (kGeoIV, SGS 211.58) demnach gelöscht werden.

Wenn das Blurring rasch erfolgt und danach nur wenige Personen der Behörde befristet Zugriff auf die Originalbilder mit Personendaten haben, ist das Risiko einer Persönlichkeitsverletzung nach Einschätzung der ASD angemessen reduziert.

Aus Sicht der Behörde handelt es sich um Personendaten, solange ihr der Schlüssel bekannt ist und Personen erkennbar sind. Aus Sicht des Cloud-Anbieters handelt es sich auch bei den Rohdaten (ohne Blurring) nicht mehr um Personendaten, sofern die Verschlüsselung genügend sicher ist und der Schlüssel dem Cloudanbieter nicht zur Verfügung steht.

2.4 BEKANNTGABE VON NAMEN IN DER EINLADUNG ZUR BÜRGERGEMEINDEVERSAMMLUNG

Die ASD wurde von einer Gemeinde gefragt, ob es zulässig sei, bei einer Einbürgerung den Namen der Person in der Einladung zur Bürgergemeindeversammlung sowie im dazu ergangenen Beschlussprotokoll auf der Website der Gemeinde auf Wunsch des Gesuchstellers nur in abgekürzter Form bekannt zu geben.

Bei der Veröffentlichung des Namens und allfälliger weiterer Angaben zum Gesuchsteller für eine Einbürgerung durch die Bürger- oder Einwohnergemeinde handelt es sich aus Sicht der ASD um eine Bekanntgabe von Personendaten an Private nach § 18f. IDG. Nach § 3 Abs. 1 des kantonalen Bürgerrechtsgesetzes (BÜG BL, SGS 110) ist die Bürgergemeindeversammlung für die Verleihung des Gemeindebürgerrechts zuständig. Die Verleihung des Gemeindebürgerrechts ist somit eine ausdrücklich gesetzliche Aufgabe der Bürgergemeinde- oder der Einwohnergemeindeversammlung. Um diese Aufgaben zu erfüllen, kann der Bürger- bzw. der Gemeinderat nach diesem Gesetz die Personendaten der Gesuchstellenden bearbeiten (vgl. § 17 Abs. 2 BÜG BL). Dies kann mittels Traktandenliste oder durch Veröffentlichung im amtlichen Publikationsorgan erfolgen, mit dem Ziel, die Stimmberechtigten über den Bewerber zu informieren. Dabei kann es sich um Angaben handeln wie Name und Vorname, Geschlecht, Geburtsjahr, Staatsangehörigkeit und die Niederlassungsdauer in der Schweiz, im Kanton und in der Gemeinde (vgl. § 17 Abs. 3 BÜG BL). § 17 Abs. 3 BÜG BL ist eine «Kann-Bestimmung». Es liegt demnach im Ermessen des Bürger- bzw. Gemeinderats, die Personendaten des Gesuchstellers den Stimmberechtigten bekannt zu geben. Im Rahmen der Ermessensausübung ist der Zweck von § 17 Abs. 3 BÜG BL (Informationsrecht der Stimmberechtigten über die Einbürgerungsdaten) mit dem Interesse des Gesuchstellers in Einklang zu bringen. Die ASD gab der Gemeinde die Auskunft, dass die gegensätzlichen Interessen gewahrt sind, wenn in der schriftlichen, nicht im Internet veröffentlichten Einladung zur Bürgergemeindeversammlung der Name des Gesuchstellers in abgekürzter Form, zum Beispiel M. Müller, angegeben ist. Hingegen bedürfen die Personendaten bei der nicht adressierten Veröffentlichung der Einladung auf der Website der Gemeinde eines höheren Schutzes. Dieser Schutz ist eher gewährleistet, wenn nur die Initialen, wie M. M., veröffentlicht werden.

Was die Bekanntgabe der Einbürgerungsdaten im Beschlussprotokoll betrifft, ist der ASD keine gesetzliche Grundlage bekannt, die das öffentliche Organ dazu verpflichtet oder ermächtigt oder dies zur Erfüllung einer gesetzlichen

Aufgabe als erforderlich erachte. Aus Sicht der ASD besteht auch keine Notwendigkeit, den Namen des Gesuchstellers im Beschlussprotokoll zu veröffentlichen. Andernfalls ist vorab die Einwilligung des Gesuchstellers zur Bekanntgabe seiner Daten einzuholen (vgl. § 18 Abs. 1 Bst. c IDG).
Auch wenn davon ausgegangen werden muss, dass eine zuverlässige Löschung im Internet nicht möglich ist, sollte die Gemeinde beachten, dass die Personendaten des Gesuchstellers im Internet gelöscht werden müssen, sobald der Zweck der Veröffentlichung erfüllt ist. Dies ist dann der Fall, wenn die Frist von 30 Tagen für die Ergreifung eines fakultativen Referendumsbegehrens gegen Beschlüsse der Gemeindeversammlung gemäss § 49 Abs. 2 des Gemeindegesetzes (GemG, SGS 180) i.V.m. § 91 des Gesetzes über die politischen Rechte (GpR, SGS 120) verstrichen ist.

2.5 BEKANNTGABE DER HERKUNFTSLÄNDER VON ASYLBEWERBERN DER GEMEINDE

Die ASD wurde von einer Gemeinde angefragt, ob es zulässig sei, einem anfragenden Dorfchronisten Herkunftsländer und Anzahl der Asylbewerber in einer Gemeinde für die Veröffentlichung in einem Zeitschriftenartikel bekannt zu geben.
Die ASD erklärte, dass bei einer solchen Bekanntgabe zu beachten sei, dass grundsätzlich alle Informationen, die in Erfüllung einer öffentlichen Aufgabe bei einer staatlichen Stelle vorhanden seien, Gegenstand eines Informationszugangsgesuches nach § 23 IDG sein könnten, soweit dem im konkreten Fall keine Einschränkungs- und Verweigerungsgründe gemäss § 27 IDG entgegenstünden.
§ 27 Abs. 3 Bst. a IDG besagt, dass ein überwiegendes privates Interesse das Zugangsgesuch einschränkt, wenn es den Schutz der Privatsphäre beeinträchtigt. Dies müsste die Gemeinde prüfen. Soweit sich der Zugang hier aber nur auf anonymisierte Personendaten richtet, also Informationen ohne Bezug zu einer bestimmten oder bestimmbaren Person, sieht die ASD grundsätzlich keine Hindernisse zur Gewährung des Zugangs. Im konkreten Fall ist aber darauf zu achten, dass aufgrund der geringen Personenzahl nicht doch aus dem Zusammenhang heraus konkrete Rückschlüsse auf eine einzelne Person gezogen werden können. Davon kann dann ausgegangen werden, wenn bei einer Personenanzahl von unter fünf dies als Information für die Bestimmbarkeit einer Person ausreichend ist. In diesen Fällen kann aber beispielsweise die Zuordnung einer Personengruppe zu einer Herkunftsregion den konkreten Personenbezug verhindern bzw. die Anonymisierung der Personendaten ermöglichen. So wird die erforderliche Anonymisierung der Personendaten nach § 28 IDG gewährleistet, wodurch der Schutz der Privatsphäre sichergestellt ist. Unter diesen datenschutzrechtlichen Erwägungen sieht die ASD einen Zugang zu den anonymisierten Informationen als zulässig.

2.6 BEKANNTGABE VON STEUERDATEN AN DIE GEMEINDERÄTE

In einer Gemeinde ersuchte der Gesamtgemeinderat um einen Bericht der Verwaltung über die 10 besten Steuerzahler der Gemeinde. Der Gemeinderat begründete dies damit, dass man so besser abschätzen könne, was ein Wegzug eines guten Steuerzahlers bedeuten würde.
Ein öffentliches Organ darf Personendaten nur bekannt geben, wenn dies in einer gesetzlichen Grundlage vorgesehen, zur Erfüllung einer gesetzlichen Aufgabe notwendig ist oder wenn eine Einwilligung der betroffenen Person(en) vorliegt. Dies gilt auch für den Austausch von Personendaten zwischen öffentlichen Organen. Das IDG geht von einem funktionalen Behördenbegriff aus: Eine Gemeinde besteht somit aus mehreren öffentlichen Organen. Diese sind organisatorisch nach Aufgabengebieten getrennt. Auch der (Gesamt-) Gemeinderat stellt ein einzelnes öffentliches Organ mit gesetzlich vorgegebenen Aufgaben dar.
Auf dieser Grundlage beantwortete die ASD die Fragestellung wie folgt (wobei sie annahm, dass keine Einwilligungen der Steuerzahler vorlagen):
Es ist durchaus eine Aufgabe der Finanzverwaltung der Gemeinde, allfällige Risiken betreffend eine mögliche Veränderung des Steuersubstrats zu evaluieren. Unbestritten (bzw. notwendig) scheint zudem, dass auch der zuständige Gemeinderat – im Rahmen seiner Aufgaben als Finanzvorsteher – Einblick in diese Informationen nehmen darf/muss. Anders liegt der Fall des Gremiums «Gesamtgemeinderat». Es ist aus Sicht der ASD nicht nachvollziehbar, zur Erfüllung welcher (gesetzlich vorgegebenen) Aufgabe des Gesamtgemeinderats dieser wissen muss, welche Personen innerhalb der Gemeinde die meisten Steuern bezahlen. Vielmehr scheint eine anonyme Auflistung der Steuerbeträge (bzw. der prozentualen Einkünfte der Gemeinde pro Steuerzahler) als ausreichend, um allfällige Massnahmen treffen zu können. Wenn die zuständige Abteilung der Gemeinde eine Anonymisierung der Daten der Steuerpflichtigen vornimmt, das heisst ohne Merkmale, die einen Personenbezug herstellen lassen, bleibt zudem auch das spezialgesetzliche Steuergeheimnis gewahrt.

2.7 DATENSCHUTZ IM GROSSRAUMBÜRO

Die ASD erreichten im Berichtsjahr mehrere Anfragen betreffend die datenschutzrechtlichen Anforderungen an Grossraumbüro-Umgebungen mit einer flexiblen Arbeitsplatzgestaltung. Solche Bürokonzepte umfassen typischerweise verschiedene Zonen, wie offene Bereiche für Teamarbeit, Ruhezonen für konzentriertes Arbeiten, Telefon- oder Videokonferenzräume, Besprechungsräume, geteilte Arbeitsplätze (Shared Desks) sowie feste Arbeitsplätze.
Wenn Mitarbeitende mit unterschiedlichen Aufgabenbereichen räumlich eng zusammenarbeiten, bringt dies datenschutzrechtliche Herausforderungen mit sich. Die Kenntnis von personenbezogenen Informationen ist für jede mitarbeitende Person auf das für ihre Aufgabenerfüllung Notwendige zu beschränken (vgl. § 9 IDG). Aus der Tatsache, dass alle Mitarbeitenden öffentlicher Organe dem Amtsgeheimnis unterstellt sind, folgt nicht, dass personenbezogene Informationen intern frei zugänglich sein dürfen. Selbst Mitarbeitende der gleichen Behörde – Vertretungssituationen vorbehalten – sind untereinander an die Schweigepflicht gebunden. Die Schweigepflichten, wie das allgemeine Amtsgeheimnis oder spezialgesetzliche Geheimhaltungsbestimmungen, wirken somit nicht nur gegen aussen, also Dritten gegenüber, sondern auch innerhalb der Behörden.
Es sind somit technische und organisatorische Massnahmen zu ergreifen, um die Informationen über Personen angemessen vor unberechtigter Kenntnisnahme zu schützen. Hierzu hat die ASD unter anderem folgende Empfehlungen abgegeben.

Räumlichkeiten

Grundsätzlich empfiehlt die ASD, Arbeitsplätze so zu gestalten, dass nur Mitarbeitende Informationen zu Personendaten haben, die diese zur Erfüllung ihrer Aufgabe benötigen. Daraus ergeben sich konkrete Massnahmen:

- Wie bei allen Büroräumlichkeiten ist auch in Grossraumbüros der Zugang zu schützen. Dies kann zum Beispiel mit personalisierten Badges für berechtigte Mitarbeitende am Eingang der jeweiligen Bürozone erfolgen.
- Um den Zugang für Besucher auf Bereiche zu beschränken, in denen keine Personendaten digital oder auf Papier bearbeitet werden, sollten sich beispielsweise Sitzungszimmer ausserhalb der Büroumgebung befinden. Für Besucher, die dennoch die Büroumgebung betreten müssen, empfiehlt die ASD das Standardvorgehen (Begleitung, sichtbarer Ausweis etc.).
- Um die Vertraulichkeit zu wahren, sollten Massnahmen zum Schall- und Sichtschutz umgesetzt werden. Dies grenzt die Möglichkeit zur Einsicht auf die Bildschirme der Mitarbeitenden ein und minimiert die Hörbarkeit von fremden Telefongesprächen.

Besondere Beachtung ist beim Umgang mit streng vertraulichen (Personen-)Daten in Grossraumbüro-Umgebungen folgenden Punkten beizumessen:

- Für Gespräche, bei welchen streng vertrauliche Personendaten ausgetauscht werden, empfiehlt die ASD, dass geeignete Räume (Telefonzellen, Vertraulichkeitszonen) zur Verfügung stehen, damit ausgewichen werden kann.
- Physische Akten mit Personendaten sind sicher zu verwahren. Dafür müssen abschliessbare Aufbewahrungsmöglichkeiten vorhanden sein.
- Eine «Clean Desk Policy» ist auch tagsüber zu befolgen.
- Bei jedem Verlassen des Arbeitsplatzes ist der Computer zu sperren.

Zudem empfiehlt die ASD, die Mitarbeitenden gezielt für die spezifischen Risiken zu sensibilisieren, die sich aus der Arbeit in einer Grossraumbüro-Umgebung ergeben.

2.8 DURCHBRECHUNG EINER DATENSPERRE

Eine Gemeinde gelangte an die ASD mit der Bitte um Einschätzung, ob eine Datensperre durchbrochen werden dürfe. Jede Person hat das Recht, beim verantwortlichen öffentlichen Organ die Bekanntgabe ihrer Personendaten schriftlich sperren zu lassen (§ 26 Abs. 1 IDG). Eine Datensperre kann dann Sinn machen, wenn bei öffentlichen Verwaltungsstellen Personendaten bearbeitet werden, welche auch der Öffentlichkeit grundsätzlich zugänglich gemacht werden können, aber nicht müssen. Dies ist etwa der Fall beim Einwohnerregister der Gemeinden, bei der MFK (Zuordnung des Kontrollschilds auf den Halter) sowie dem (elektronischen) Grundbuch.
Eine Bekanntgabe gesperrter Daten ist gemäss § 26 Abs. 2 IDG nur möglich, wenn alternativ das öffentliche Organ zur Bekanntgabe gesetzlich verpflichtet ist, die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder wenn die um Bekanntgabe ersuchende Person glaubhaft macht, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind.

Im konkreten Fall wurde ein Vermieter einer Wohnung bei den Einwohnerdiensten der Gemeinde vorstellig und verlangte die neuen Adressdaten des vormaligen Mieters, da noch Schulden aus dem Mietverhältnis bestehen würden. Der (vormalige) Mieter hatte bei den Einwohnerdiensten eine Datensperre hinterlegt. Angesichts der Datensperre und der Tatsache, dass der Vermieter nur einen nicht mehr aktuellen Mietvertrag vorgelegt hatte, war man sich bei der Gemeinde nicht schlüssig, ob die Rechtslage erlaube, die gewünschten Adressdaten herauszugeben.
Die ASD stellte fest, dass vorliegend weder eine gesetzliche Pflicht bestehe, die Daten weiterzugeben, noch dass dies zur Aufgabenerfüllung (der Verwaltung) notwendig sei. Eine Durchbrechung der Datensperre kann nur erfolgen, wenn die anfragende Person glaubhaft macht, dass die Informationen für die Durchsetzung ihrer Rechtsansprüche notwendig sind. Gerade im Bereich der Betreibung von Schulden kann ein solcher Rechtsanspruch bestehen. Daher ist durch die Verwaltungsstelle zu klären, ob das Bestehen eines Rechtsanspruchs glaubhaft ist. Ein Mietvertrag kann zum Beispiel durchaus ein Hinweis auf Rechtsansprüche sein, ein Beleg, dass Schulden bestehen, ist er aber nicht. Massstab ist vorliegend eine «Glaubhaftmachung» eines Anspruches. Glaubhaft erscheint dabei eine Behauptung, wenn mehr Anhaltspunkte für das Vorliegen einer Tatsache sprechen als dagegen. Wichtig und zentral ist dabei die Mitwirkungspflicht des Antragstellers.
Es muss allerdings auch betont werden, dass die Gemeindeverwaltung nicht die Funktion hat, anstelle eines Gerichts die Berechtigung des Anspruchs zu beurteilen. Es geht bei dieser Prüfung somit insbesondere darum, sicherzustellen, dass sich eine gesperrte Adresse nicht mit einer fadenscheinigen Begründung verschafft wird, was zum Beispiel in Stalking-Situationen schwere Folgen für die betroffene Person haben kann. Aus diesem Grund muss der betroffenen Person die Möglichkeit gegeben werden, zum Gesuch Stellung nehmen zu können.

2.9 ANFRAGEN ZU M365

Immer mehr Gemeinden befassen sich mit der Frage, ob sie von ihren lokal installierten Office-Umgebungen auf Cloud-basierte M365 wechseln sollen oder gar müssen. Oft ist der Wunsch nach Delegation des Office-Betriebs verbunden mit der Hoffnung, damit auch die Verantwortung an die externe Dienstleisterin abgeben zu können. Dabei sehen sie primär die von der Anbieterin kommunizierten Vorteile wie «Skalierbarkeit, Mobilität, automatische Updates». Dass den genannten Vorteilen auch Nachteile oder im öffentlich-rechtlichen Umfeld gar rechtliche Einschränkungen entgegenstehen, wird im ersten Moment gerne übersehen.
Ein wesentlicher Bestandteil einer Analyse der «Datenschutztauglichkeit» von allen Outsourcing-Lösungen ist die Prüfung betreffend Erfüllung der Anforderungen aus dem Merkblatt «Datenbearbeitung im Auftrag» (i.S.v. § 7 IDG). Im Speziellen ist bei Cloud-Lösungen zudem das Merkblatt «Cloud-spezifische Risiken und Massnahmen» von privatim (Konferenz der schweizerischen Datenschutzbeauftragten) zu beachten (vgl. auch Tätigkeitsbericht 2023 der ASD). Im Übrigen ist die Nutzung von Cloud-Services für Personendaten bei Behörden aufgrund der besonderen Risiken vorab konsultationspflichtig (§ 12 IDG).
Die Einwohnergemeinde bzw. der entsprechende Gemeinderat verantwortet den Einsatz von IT-Werkzeugen für ihre Verwaltung – auch bei Outsourcing (§ 7 IDG) müssen die datenschutzrechtlichen Vorgaben (Recht und Informationssicherheit) eingehalten werden. Da in Gemeinden auch besondere Personendaten bearbeitet werden, geht die ASD aktuell davon aus, dass auf der aktuellen Basis und ohne entsprechende Verschlüsselungsmöglichkeiten M365 in der Cloud aufgrund des zu hohen Restrisikos nicht flächendeckend genutzt werden kann. Die ASD geht wie andere DSBs aktuell davon aus, dass auch mit Zusatzverträgen wie jenen mit der Digitalen Verwaltung (ehemals SIK) und Educa das Bearbeiten von besonderen Personendaten ein zu hohes Risiko birgt. Bei besonderen Personendaten wäre eine echte Ende-zu-Ende-Verschlüsselung nötig, welche aber out of the box nicht möglich ist. Auch die «Customer Lockbox» und «Bring Your Own Key»-Angebote von Microsoft können den Zugriff nur begrenzt einschränken. Die Customer Lockbox ist letztlich ein vertragliches Versprechen und nicht vergleichbar mit expliziter technischer Zugriffseinschränkung von Dritten auf On-Premises-Lösungen.
Organisatorische Weisungen, Office 365 aus der Cloud nicht für besondere Personendaten zu nutzen, erscheinen im Arbeitsumfeld von Gemeinden nicht praktikabel und bergen das Risiko, dass solche Daten trotzdem in der Public Cloud bearbeitet werden.
Die ASD empfiehlt jeweils, nach risikoärmeren Alternativen zu suchen, denn grundsätzlich darf die Auslagerung von Datenbearbeitungen für die Grundrechte der betroffenen Personen nicht nachteilig sein (vgl. Merkblatt privatim).
Nicht zuletzt gilt es zu bedenken, dass aktuell der Einsatz von M365 aus der Cloud im Office-Bereich auch nicht alternativlos ist: Denn selbst wenn man nicht auf alternative

Office-Anwendungen umstellen will, können die MS-Office-Produkte (Word, Excel etc.) auch weiterhin lokal (direkt auf dem Client) statt aus der Cloud genutzt werden.

2.10 PARKRAUMBEWIRTSCHAFTUNG

Eine Gemeinde führte per Anfang des Berichtsjahres ein System zur Parkraumbewirtschaftung ein, wo beim Parkieren auf den öffentlichen Parkplätzen im Siedlungsgebiet das Kontrollschild und die Ankunftszeit sowohl beim kostenlosen Kurzzeitparkieren als auch beim gebührenpflichtigen Parkieren digital oder an einem Parkautomaten angegeben werden müssen. Die ASD wurde von Privatpersonen angefragt, ob die elektronische Registrierung der Kontrollschilddaten beim kostenlosen Kurzzeitparkieren datenschutzkonform sei.
Für diese Art der Datenbearbeitung bedarf es gemäss § 9 IDG entweder einer gesetzlichen Grundlage oder sie muss zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Die gesetzliche Aufgabe und die damit verbundenen Ziele der neuen Parkraumbewirtschaftung wurden von der Gemeinde in einem Reglement (ein formell-gesetzlicher Erlass der Gemeinde) festgelegt. Demnach ist Ziel der neuen Parkraumbewirtschaftung, dass der beschränkte öffentliche Parkraum nur zweck- und ordnungsgemäss genutzt werden soll. Die Registrierung dient dabei dazu, die Zeitüberschreitungen beim kostenlosen Parkieren ab zwei Stunden einfach und schnell zu büssen, indem die Eingabezeit der Kontrollschilder ausgelesen werden kann.
Die ASD sah die Voraussetzungen für die damit verbundene Datenbearbeitung zur Aufgabenerfüllung als gegeben an, betonte aber, dass die Aufbewahrungsdauer der Kontrollschilddaten verhältnismässig auszugestalten sei. Die Daten müssen demnach nach Zweckerreichung umgehend gelöscht bzw. bei einer allfällig beabsichtigten Weiterverwendung für statistische Zwecke vorab anonymisiert werden. Die Gemeinde sicherte dies der ASD zu und bestätigte die Anonymisierung der Fahrzeugdaten von Kurzzeitparkierenden nach 24 Stunden.

2.11 KOMMUNIKATIONSLÖSUNGEN IM SCHULUMFELD

Der ASD wurde von einer Primarschule die Datenschutzkonformität einer Kommunikationslösung zur Prüfung vorgelegt. Ähnliche Vorhaben gab es in der Vergangenheit mehrere. Das Bedürfnis, sich mittels eines digitalen Tools rasch und einfach austauschen und schulrelevante Informationen übermitteln zu können, ist sowohl bei den Erziehungsberechtigten als auch bei den Schulbehörden vorhanden. Derzeit fehlt indessen eine gesetzliche Grundlage, die es Schulen ermöglichen würde, den Erziehungsberechtigten die Verwendung eines spezifischen digitalen Kommunikationskanals verbindlich vorzuschreiben. Digitale Tools können somit nur mit der Zustimmung der Erziehungsberechtigten verwendet werden, für den Fall, dass jemand nicht einverstanden ist, muss für diese Person ein alternativer Weg gesucht werden.
Die Tatsache, dass die Verwendung eines Kommunikationskanals auf freiwilliger Basis erfolgt, bedeutet allerdings nicht, dass die Schulen keine Pflicht haben, sich um den Schutz der darüber bearbeiteten Personendaten zu kümmern. Die datenschutzrechtliche Verantwortung verbleibt bei der Schule und somit gilt auch für diesen Fall, dass die Informationen gemäss § 8 IDG angemessen zu schützen sind. Demzufolge muss die Schule, die eine bestimmte Kommunikationslösung einsetzen will, zuerst das Risiko der Verwendung ermitteln und dann geeignete Massnahmen treffen, damit das Restrisiko tragbar wird.

Folgende Faktoren sind unter anderem bei der Risikobeurteilung zu berücksichtigen: Für welche Anwendungsfälle soll das Tool eingesetzt werden und welche Informationen sollen damit ausgetauscht werden? Da die fraglichen Tools in der Regel im Rahmen einer Auftragsdatenbearbeitung genutzt werden: Wie sieht die vertragliche Situation aus? Ist zum Beispiel die Zweckbindung sichergestellt und bedingt sich die Auftragsdatenbearbeiterin keine Verwendung der Personendaten zu eigenen Zwecken aus? Welche technischen und organisatorischen Massnahmen ergreift die Dienstleisterin? Welche können/müssen seitens der Schule ergriffen werden?

In der Regel liegen bei der Verwendung von Kommunikationstools eine Reihe von Risikofaktoren vor, die in der Summe ein hohes Risiko für die betroffenen Personen darstellen. Damit sind die Voraussetzungen für die Durchführung einer Vorabkonsultation erfüllt.

2.12 ZUGRIFF AUF PERSONALDOSSIERS

Eine Mitarbeiterin einer privatrechtlichen Stiftung, welche für eine Gemeinde öffentliche Aufgaben wahrnimmt, stellte fest, dass – nach einer Änderung in den Zugriffsberechtigungen – alle Personaldossiers für sämtliche Mitarbeitenden offen einsehbar waren. Sie wollte wissen, ob dies mit den datenschutzrechtlichen Bestimmungen vereinbar sei. Bei

Anfragen muss die ASD immer zuerst ihre Zuständigkeit klären. In der genannten Konstellation gilt die Stiftung gemäss § 3 Abs. 1 Bst. c IDG als öffentliches Organ, soweit ihr die Erfüllung öffentlicher Aufgaben übertragen wurde. Damit will der Gesetzgeber sicherstellen, dass die Regeln zur staatlichen Datenbearbeitung auch dann greifen, wenn diese durch Private erfolgt. Im Blick hatte er dabei aber nicht die privatrechtlich angestellten Mitarbeitenden des Privaten, sondern die Personen, deren Datenbearbeitung mit der Erfüllung der öffentlichen Aufgabe direkt verknüpft ist – wie die Patienten einer Privatklinik auf der Spitalliste. Aus diesem Grund kommt die ASD im Bereich des Personals einer privaten Organisation zum Schluss, dass sie nicht zuständig ist und somit nicht tätig werden darf. Zuständig ist damit der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

Dennoch konnte die ASD der anfragenden Person mitteilen, dass sie einen vergleichbaren Fall innerhalb ihres Zuständigkeitsbereichs als klaren Verstoss gegen die Bestimmungen des IDG werten würde, da durch die vollständige Offenlegung der Personaldossiers das «Need-to-know-Prinzip» offensichtlich nicht beachtet wird. Es ist allerdings davon auszugehen, dass der eingetretene Fall als Folge der Änderung der Berechtigungen ungewollt erfolgte. Eine erhöhte Gefahr für ungewollte datenschutzrelevante «Nebeneffekte» besteht insbesondere nach einem neuen Release einer Software. Zur datenschutzrechtlichen Verantwortung des öffentlichen Organs gehört es, die Einstellungen von Anwendungen, die das Need-to-know-Prinzip umsetzen, periodisch sowie nach Releases zu überprüfen.

Nur der Vollständigkeit halber sei darauf hingewiesen, dass eine derartige Datenschutzverletzung meldepflichtig ist (§ 15a IDG).

3

VORABKONSULTATION

Das Ziel der Vorabkonsultation ist seit ihrer Einführung im Jahr 2008, Anforderungen des Datenschutzes frühzeitig zu berücksichtigen, um für eine rechtmässige Bearbeitung im Betrieb zu sorgen.
Die ASD stellt für die Datenschutz-Folgenabschätzung (DSFA) und die Vorabkonsultation Hilfsmittel zur Verfügung: die Checkliste DSFA/Vorabkonsultation (Schwellwertanalyse) und den Leitfaden DSFA / Vorabkonsultation.

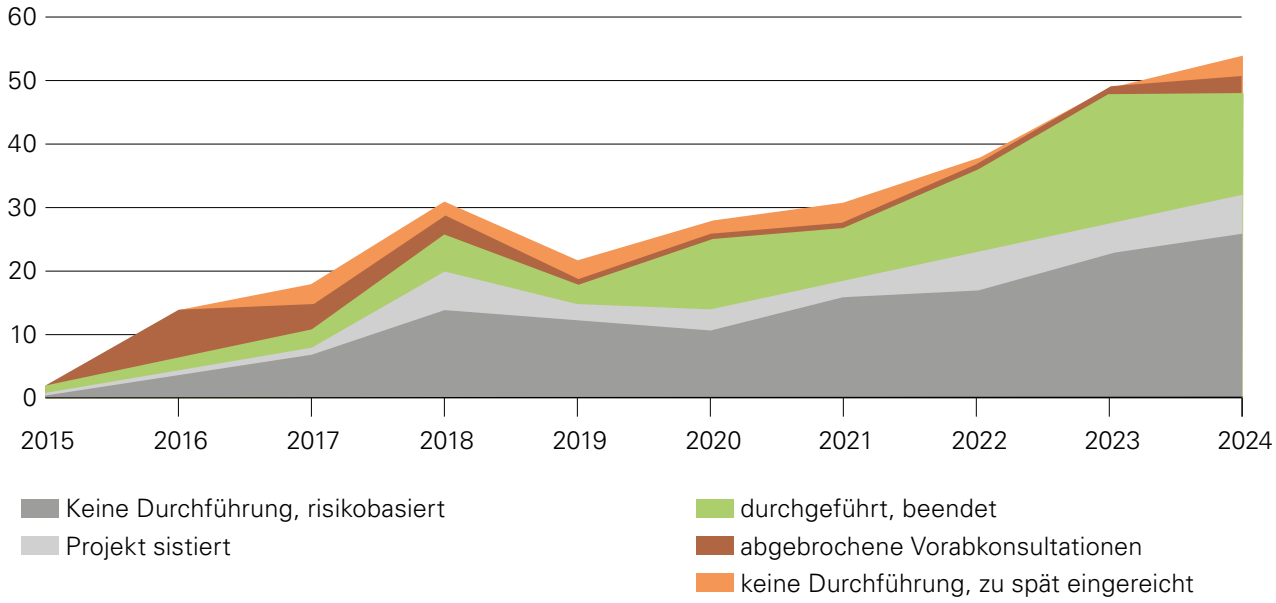
Der Pflicht zur Vorabkonsultation unterliegen demnach:

- Rechtsetzungsprojekte zur Bearbeitung von Personendaten,
- Vorhaben, die aufgrund der zu bearbeitenden Daten voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, und
- Vorhaben, bei denen die Art der Datenbearbeitung voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen bewirkt. Dies betrifft insbesondere die Verwendung neuer Technologien oder Funktionserweiterungen, welche neue oder zusätzliche Informationen generieren (bspw. Patientenportal, Internet der Dinge, Videoberatung usw.) oder angepasste Massnahmen für die Gewährleistung der Informationssicherheit erfordern (bspw. Auftragsdatenbearbeitung).

Im Rahmen der Vorabkonsultation einer geplanten Datenbearbeitung wird geprüft, ob das verantwortliche 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 Vorabkonsultation vorgelegten Projekte unterscheiden sich bezüglich Tragweite, Komplexität, eingesetzter Technologie und damit verbundener Risiken stark voneinander. Die Aufsichtsstelle prüft nicht alle ihr vorgelegten Projekte, die Selektion erfolgt risikobasiert. Die ASD hält die Durchlaufzeiten grundsätzlich so kurz wie möglich. Immer häufiger wird das Angebot der ASD einer möglichst frühen Kontaktaufnahme genutzt und ermöglicht dadurch die Durchführung des Prüfprozesses in mehreren Einzelschritten.
Im Berichtsjahr wurden der ASD 74 Projekte neu zur Vorabkonsultation eingereicht. Zu 23 davon hat die ASD aufgrund ihrer Risikobeurteilung keine Vorabkonsultation durchgeführt. Ein Projekt wurde noch während der Vorabkonsultation in Betrieb genommen, bevor die Stellungnahme der ASD vorlag. Zehn Stellungnahmen betrafen die Vorabkonsultationspflicht von Rechtsetzungsprojekten betreffend die Bearbeitung von Personendaten, die seit der IDG-Revision vom 1. Januar 2022 gilt (§ 12 Abs. 1 Bst. a). Diese erfolgten mehrheitlich im Rahmen des ordentlichen Mitberichtsverfahrens.
Die Vorabprüfungen von Digitalisierungsprojekten, E-Government-Vorhaben – immer häufiger unter Einbezug von Cloud-Services – und überkantonalen Fachanwendungen bildeten die Schwerpunkte im Berichtsjahr.

Entwicklung der zur Vorabkonsultation vorgelegten Vorhaben nach Abschlussjahr:

ENTWICKLUNG VORABKONSULTATIONEN



Die gesetzliche Pflicht, die geplante Datenbearbeitungen abhängig vom Risiko der ASD zur Prüfung vorzulegen, besteht seit 2008. Vor 2015 wurden nur wenige Projekte zur Vorabkontrolle eingereicht. Im April 2015 publizierte die ASD die erste Ausgabe des Leitfadens zur Vorabkontrolle, welcher sowohl den Projektverantwortlichen als auch den verantwortlichen Organen als Unterstützung bei der Triage und der Einbettung der Vorabkontrolle in den Projektablauf dient. Dabei wurde damals wie heute grosser Wert darauf gelegt, auf die im Kanton bereits standardisierte Projektmethode HERMES aufzubauen.
Die Auswertung zu den eingegangenen Vorabkonsultationen zeigt, dass das Bewusstsein um die gesetzliche Pflicht stark zugenommen hat. Ausserdem ist sichtbar, dass nur vereinzelte Behörden eine Vorabkonsultation abbrechen, indem sie während der Prüfung durch die ASD die Inbetriebnahme starten. Eine zunehmende Anzahl Vorabkonsultationen kann mit einer von der Behörde zugesicherten Nachbesserung beendet werden.

4

KONTROLLTÄTIGKEIT

Gemäss § 40 Bst. a IDG kontrolliert die ASD 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 Prüfung der vor Ort umgesetzten Massnahmen. Anders als bei der präventiven Vorabkonsultation in der Konzeptionsphase wird hier die Einhaltung der Vorgaben im laufenden Betrieb geprüft. Die ASD pflegt eine rollende, risikobasierte Kontrollplanung. Ebenfalls zur Kontrolltätigkeit zählt die Analyse der Umsetzung von Empfehlungen nach erfolgten Kontrollen. Die ASD geht davon aus, dass ihre Empfehlungen der Dringlichkeit entsprechend in angemessener Frist, in der Regel nach zwölf Monaten, umgesetzt werden. Ziel der Kontrollen ist neben den konkreten Erkenntnissen zum Handlungsbedarf immer auch eine Sensibilisierung hinsichtlich des 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. Schwierig gestaltet sich jeweils die Umsetzung von Empfehlungen, wenn diese eine Lösung betreffen, die als Kooperationslösung in verschiedenen Kantonen oder Städten eingesetzt wird, die Verantwortung für die rechtmässige und angemessene sichere Datenbearbeitung jedoch bei der jeweiligen Behörde liegt. Die ASD nutzt hier fallweise die Konferenz der Datenschutzbeauftragten (privatim), um koordinierend zu unterstützen.

4.1 KONTROLLE EINER KLINIK

Die für die Kontrolle ausgewählte Privatklinik bearbeitet zahlreiche Personendaten mit Angaben über die Gesundheit. Diese stellen besondere Personendaten im Sinne von § 3 Abs. 4 IDG dar. Die geprüfte Klinik erbringt medizinische Leistungen gemäss den bundesrechtlichen und kantonalen Vorgaben. Der Umfang der Aufgaben, welche sie in Erfüllung ihres öffentlichen Auftrags wahrnimmt, ergibt sich aus der kantonalen Spitalliste. Im Rahmen dieser Aufgabenerfüllung untersteht sie den Bestimmungen des IDG und der Aufsicht der ASD. Die Klinik ist bei der Bearbeitung von Personendaten nach § 6 Abs. 1 IDG verantwortlich für die Einhaltung der Vorgaben des IDG, welche durch die einschlägigen Bestimmungen der Fachgesetze, insbesondere des Krankenversicherungsgesetzes vom 18. März 1994 (KVG, SR 832.10), ergänzt werden.

Schwerpunkte dieser Datenschutzkontrolle bildeten die Rechtmässigkeit und die Verhältnismässigkeit der Erhebung der Personendaten bei Kontaktaufnahme mit Klienten sowie die Bearbeitungsvorgänge während der Behandlung, die Verantwortlichkeiten, die Erkennbarkeit der Datenbearbeitung, die Aufbewahrung und Vernichtung der Daten und die sich stellenden Herausforderungen bei einer Auslagerung der Datenbearbeitung an externe Auftragsdatenbearbeiter. Geprüft wurden auch die technischen und organisatorischen Massnahmen betreffend die Informationssicherheit.

Die Kontrolle ergab, dass das Bewusstsein der Klinik für die datenschutzrechtlichen Pflichten in hohem Masse vorhanden war. Handlungsbedarf sah die ASD insbesondere bei Passwortvergabe und -einstellungen, Zugriffsberechtigungen sowie beim Thema der Vernichtung von nicht mehr benötigten Personendaten. Ebenfalls Handlungsbedarf sah die ASD bei der Zugänglichkeit zu den Patientendossiers in Papierform.

Die Klinik hat bestätigt, dass sie die Empfehlungen der ASD akzeptiert und sie umsetzen wird.

4.2 KONTROLLE EINER STIFTUNG MIT LEISTUNGSAUFTRAG IM BEREICH DER SUCHTPRÄVENTION UND BERATUNG

Die durch die ASD geprüfte Stiftung ist eine Organisation mit mehreren Standorten im Kanton Basel-Landschaft.

Der Stiftung sind mit einer Leistungsvereinbarung vom Kanton Basel-Landschaft kantonale gesetzliche Aufgaben nach § 69 Abs. 3 Gesundheitsgesetz (GesG, SGS 901) übertragen worden. Die Stiftung bietet ambulante Abklärung, Therapie, Beratung, Begleitung, Stütze und Information für Betroffene, deren Angehörige, Bezugspersonen oder Arbeitgebende, welche direkt oder indirekt betroffen sind, an. Das Angebot richtet sich dabei ausschliesslich an Einwohnerinnen und Einwohner des Kantons Basel-Landschaft.

Nach § 6 Abs. 1 IDG trägt dasjenige Organ die Verantwortung für den Umgang mit Informationen, das diese zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. Diese Verantwortung können auch private Dritte tragen, soweit ihnen wie hier vom Kanton die Erfüllung öffentlicher Aufgaben übertragen wurde.

Schwerpunkte dieser Datenschutzkontrolle bildeten die Rechtmässigkeit und die Verhältnismässigkeit der Erhebung der Personendaten bei Kontaktaufnahme mit Klienten sowie die Bearbeitungsvorgänge während der Betreuung, die Verantwortlichkeiten, die Erkennbarkeit der Datenbearbeitung, die Aufbewahrung und Vernichtung der Personendaten und die sich stellenden Herausforderungen bei einer Auslagerung der Datenbearbeitung an externe Auftragsdatenbearbeiter. Geprüft wurden auch die technischen und organisatorischen Massnahmen betreffend die Informationssicherheit.

Handlungsbedarf identifizierte die ASD insbesondere bei den vertraglichen Vereinbarungen mit den Auftragsdatenbearbeiterinnen, Modalitäten bei Gefährdungsmeldungen, der Benutzerverwaltung, Passworteinstellungen, dem elektronischen Klientendossier, der Terminvereinbarungssoftware, der Videokonferenzberatung sowie bei der digitalen Kommunikation mit Klienten.

Die Stiftung hat bestätigt, dass sie die Empfehlungen der ASD akzeptiert und sie umsetzen wird.

4.3 SCHENGEN-KONTROLLE

Das Schengener Informationssystem (SIS) wird von den Schengen-Staaten, zu denen auch die Schweiz zählt, gemeinsam betrieben. Das SIS enthält gespeicherte Daten über gestohlene oder gesuchte Gegenstände und Einträge zu polizeilich und gerichtlich gesuchten, mit einem Einreiseverbot belegten oder vermissten Personen. Mit der Übernahme des Schengen-Acquis verpflichtete sich die Schweiz, zu gewährleisten, dass eine unabhängige Behörde die Rechtmässigkeit der Verarbeitung personenbezogener Daten des Schengener Informationssystems (SIS) in ihrem Hoheitsgebiet und deren Übermittlung aus ihrem Hoheitsgebiet überwacht.

So sind die kantonalen Datenschutzbeauftragten gehalten, periodisch die Rechtmässigkeit der Bearbeitung personenbezogener Daten im SIS zu kontrollieren (Art. 69 Verordnung [EU] 2018/1862 in Verbindung mit Art. 8b des Bundesgesetzes über die polizeilichen Informationssysteme [BPI, SR 361]).

Im Kanton Basel-Landschaft weist die kantonale Polizei die grösste Anzahl an SIS-abfrageberechtigten Personen auf und wurde deshalb im Berichtsjahr für die Kontrolle ausgewählt.

Die ASD hat anlässlich der Kontrolle festgestellt, dass die Nutzung des SIS bzw. der nationalen Informationssysteme bei der Polizei Basel-Landschaft grundsätzlich unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgt.

Handlungsbedarf wurde unter anderem im Bereich der Sensibilisierung und Überarbeitung von Richtlinien erkannt. Damit soll das Bewusstsein für die Verantwortung für die Datenbearbeitung verstärkt und das Wissen um die Bedeutung eines sorgsamen Umganges mit besonderen Personendaten, gerade auch im Bereich der SIS-Zugriffe, erhöht werden.

Die Polizei Basel-Landschaft hat bestätigt, dass sie die Empfehlungen der ASD akzeptiert und sie umsetzen wird.

4.4 KONTROLLE ECHTDATEN ZU TEST-/SUPPORTZWECKEN

Die ASD hat bei den öffentlichen Organen im Kanton eine Datenschutzkontrolle zur Verwendung von Echtdaten (Personendaten) bei externen Dienstleistern, ausserhalb der produktiven Systeme des täglichen Betriebs, durchgeführt. Anlass für diese Prüfung waren unter anderem Cyberangriffe auf Softwarefirmen, die im Auftrag von öffentlichen Organen Personendaten bearbeiten, sowie die generell steigenden Risiken im Bereich der Cyberangriffe.

Schwerpunkte der Datenschutzkontrolle bildeten die Prüfung der Notwendigkeit und der Art der Übermittlung von Personendaten an externe Dienstleister sowie das Vorliegen schriftlicher Vereinbarungen, welche die Verwendung und Einhaltung der Zweckbindung, den Schutz sowie die sichere Vernichtung der übermittelten Personendaten regeln.

Hierzu hat die ASD den öffentlichen Organen Fragebögen zugestellt, welche im Rahmen eines «Self-Assessments» beantwortet wurden. Die Feststellungen der ASD basierten auf der Analyse der erhaltenen Antworten. Die ASD stellte fest, dass in einzelnen Fällen die Anforderungen bei der Einhaltung der Zweckbindung, der Art der Übermittlung von Personendaten, der Vernichtung und bei den Vereinbarungen mit den Auftragnehmerinnen teilweise nicht angemessen erfüllt werden.

Die daraus resultierenden Empfehlungen gelten nicht nur für aktuelle, sondern auch für zukünftige Datenbearbeitungen und wurden den öffentlichen Organen zugestellt. Diese prüften im Anschluss eigenständig, ob die im Bericht festgestellten Abweichungen vom Soll-Zustand auf eine oder mehrere ihrer Applikationen oder Prozesse zutreffen, und wurden aufgefordert, die entsprechenden Massnahmen umzusetzen.

5

ÖFFENTLICHKEITSPRINZIP

Die Landeskanzlei hat der ASD 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 2023	Gesuche 2024	gutgeheissen	teilweise gutgeheissen	abgewiesen
BKSD	3	3	1	1	1
BUD	2	4	0	1	3
FKD	5	1	0	0	1
SID	10	10	5	1	4
VGD	4	3	1	1	1
LKA	14	13	11	0	2
Total	**38**	**34**	**18**	**4**	**12**

Die von der Landeskanzlei erstellte Statistik weist eine gegenüber dem Vorjahr nahezu unveränderte Anzahl Gesuche um Zugang zu Informationen aus. Die Abweisungsquote liegt etwas höher, Grund dafür scheint der höhere Anteil von Gesuchen, die sich auf noch laufende Verfahren beziehen, zu sein. Die hohe Anzahl von Gesuchen in der Landeskanzlei umfassen auch Gesuche, die beim Staatsarchiv eingegangen sind. Dabei wurde mehrheitlich Zugang zu Regierungsratsbeschlüssen verlangt, welcher in aller Regel gewährt wird.

Damit scheint sich das Volumen der Zugangsgesuche auf einem Niveau eingependelt zu haben, das aus Sicht der Verwaltung bewältigbar erscheint. Dies widerspiegelt auch die Tatsache, dass bei der ASD im Berichtsjahr verhältnismässig wenige Beratungsanfragen eingingen. Dies betrifft sowohl die Privaten als auch die öffentlichen Organe.

12 Jahre nach Einführung des Öffentlichkeitsprinzips kann aus Sicht der ASD festgestellt werden, dass die damit bezweckte Transparenz «lebt», das Instrument wird genutzt, und es scheint sich ein pragmatischer Umgang etabliert zu haben, in welchem befriedigende Lösungen gefunden werden, ohne dass der Rechtsweg beschritten werden muss. So hat das Kantonsgericht bis dato nur sehr wenige Entscheide fällen müssen, im Berichtsjahr war es soweit ersichtlich gar keiner.

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.

6.2 FACHGRUPPE INFORMATIONS-SICHERHEIT (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 neben der Beratung bei aktuellen Themen auch Unterstützung bei der Erarbeitung von neuen Vorlagen betreffend Risikomanagement und ISDS-Konzeption sowie Regelungsbedarf beim Einsatz von KI-Tools bieten. Sie beriet die FIS ausserdem bei der Behandlung der Ausnahmeanträge und zeigte die damit verbundenen Risiken auf. Auch ausserhalb dieser institutionalisierten Treffen fand im Berichtsjahr ein konstruktiver Austausch mit einzelnen dezentralen und dem kantonalen Sicherheitsbeauftragten statt.

6.3 ITO-RAT

Die ASD nimmt an den Sitzungen des ITO-Rats als Gast teil. So kann sich die ASD auf dieser Ebene zu Themen des Datenschutzes und der Digitalisierung sowie zu Umgang und Bearbeitung von Personendaten einbringen.

6.4 DATENSCHUTZBEHÖRDEN ANDERER KANTONE

Die ASD arbeitete bei diversen Geschäften mit Datenschutzbehörden anderer Kantone zusammen, holte Einschätzungen zu Sachverhalten ein oder gab diese selbst ab. Auch ist sie aktives Mitglied und im Vorstand vertreten von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, welche die Grundlage für eine gute Zusammenarbeit der Datenschutzbehörden bildet und diese kontinuierlich fördert. Im Rahmen dieser Zusammenarbeit mit anderen Aufsichtsbehörden kann sie ihr Fachwissen aufrechterhalten und vertiefen sowie ihre Haltung und ihre Auslegung mit anderen Aufsichtsbehörden abgleichen. Zudem leistet privatim einen Beitrag zur Verbesserung des Datenschutzes und der Informationssicherheit.

Die für die ASD relevanten Arbeitsgruppen von privatim, in denen sie vertreten ist, werden in den folgenden Kapiteln aufgeführt.

6.5 AG ICT

Die Arbeitsgruppe ICT fördert den Austausch der Informatikerinnen und Informatikern, die bei einer Datenschutzbehörde beratend und als IT-Revisorinnen und -Revisoren arbeiten. Der Schwerpunkt im Berichtsjahr lag auf dem Austausch über konkrete Projekte und kantonsübergreifend eingesetzte Lösungen. Ausserdem tauschte sich die ASD mit einzelnen Mitgliedern zu spezifischen Vorabkonsultationen ausführlicher aus, um Synergien zu nutzen.

6.6 AG SICHERHEIT

Die Zusammenarbeit im Bereich der Arbeitsgruppe Sicherheit, die von der ASD geleitet wird, fand im Berichtsjahr fallbezogen statt. Die Koordination fand im Bereich diverser Vorabkonsultationen, die in verschiedenen Kantonen anstanden, statt. Die Mitglieder der Arbeitsgruppe wurden verschiedentlich für die Prüfung von Projektdokumenten, oftmals Verträgen, beigezogen, in welchen eine überregionale, oft nationale Komponente bestand. Die Entwicklung namentlich im Polizeibereich geht gegenwärtig in Richtung komplexer Systeme, die von mehreren oder gar einer überwiegenden Mehrheit der Kantone genutzt werden. Aufgrund der Tatsache, dass Polizeiarbeit in die kantonale Zuständigkeit fällt, stellen sich rund um solche Anwendungen eine Vielzahl Fragen zur rechtlichen Ausgestaltung. In den Medien prominent diskutiert wurden die Fragestellungen rund um den interkantonalen Austausch von Polizeidaten im Rahmen des Projekts «POLAP». Auch hier versuchte die Arbeitsgruppe Sicherheit, den Stakeholdern beratend zur Verfügung zu stehen.

6.7 AG GESUNDHEIT

Die Arbeitsgruppe Gesundheit hielt im Berichtsjahr drei ordentliche Sitzungen ab. Zudem besuchte sie eine informative Veranstaltung zum Thema des aktuellen Stands und der Einsatzmöglichkeiten von KI im Gesundheitsbereich. Zentrale Themen der Arbeitsgruppe Gesundheit waren unter anderem KI und Forschung, die Datenbearbeitung bei der Verwendung von Lifestyle/Health Apps, die Notwendigkeit von Einwilligungen im Bereich der Forschung nach

Humanforschungsgesetz oder die Regelung von (Lese-) Zugriffen auf Patientendokumentationen in grösseren medizinischen Institutionen.
Obgleich die Gesundheitspolitik grundsätzlich in den Händen der Kantone liegt und die gesetzlichen Vorgaben von Kanton zu Kanton unterschiedlich ausgestaltet sind, ist der Austausch innerhalb der Arbeitsgruppe immer gewinnbringend. Der medizinische Fortschritt und der steigende Bedarf an Gesundheitsdaten stellen alle Kantone vor ähnliche Fragestellungen und Probleme. Der Austausch in der Arbeitsgruppe Gesundheit dient daher auch dazu, sich neuer Fragestellungen bewusst zu werden. Durch den Austausch der ASD mit zuständigen Stellen des Kantons werden allfällige Probleme erkannt, teilweise aber auch vorbildliche Lösungen, welche den anderen Kantonen über die Arbeitsgruppe als mögliche Lösungsansätze vorgeschlagen werden können.

6.8 AG DIGITALE VERWALTUNG

Die Arbeitsgruppe Digitale Verwaltung traf sich im Berichtsjahr dreimal. An diesen Sitzungen wurden aktuelle Themen wie die datenschutzrechtliche Zulässigkeit und deren Voraussetzungen zur Einführung von M365 in den Kantonsverwaltungen diskutiert. Ausserdem wurde die Einführung der Justizplattform Justitia 4.0 vorgestellt, wobei durch die Anwesenheit von Personen aus den Pilotkantonen über den aktuellen Stand der Arbeiten informiert werden konnte. Über das Thema Künstliche Intelligenz, die kantonalen Entwicklungen in diesem Zusammenhang und sich daraus ergebende datenschutzrechtliche Fragen tauschte sich die Arbeitsgruppe in allen Sitzungen intensiv aus. Genauso stand ein kantonaler Austausch über vorgefallene Fälle zu Datenschutzverletzungen und die Handhabung der damit verbundenen Meldepflichten wiederholt auf dem Traktandum.

6.9 SCHENGEN-RELEVANTE GREMIEN

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 zwar vom Bund betrieben, jedoch auch von den Kantonen genutzt werden, müssen entsprechende Kontrollen zuständigkeitshalber sowohl von den kantonalen Aufsichtsstellen als auch vom 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. Die Mitglieder wurden dabei von den Vertreterinnen in den Schengen-relevanten europäischen Datenschutzgremien über die Weiterentwicklung des Schengen-Rechtsrahmens orientiert. Des Weiteren wurde über die in den Kantonen und beim Bund vorgenommenen Kontrollen informiert, wobei hier auch besonders methodologische Themen erörtert wurden.
Ein weiterer Teil der datenschutzrechtlichen Verpflichtung der Schengen-Mitgliedstaaten ist die Evaluation der Umsetzung der diesbezüglichen Gesetzgebung in den Mitgliedstaaten. Die Vor-Ort-Besuche im Rahmen der Evaluation der Schweiz wurden seitens der europäischen Kommission auf Januar 2025 terminiert, was zur Folge hatte, dass besonders in der zweiten Jahreshälfte intensive Vorbereitungsarbeiten anstanden. Die ASD nahm hier im Auftrag von privatim Einsitz in die entsprechende Arbeitsgruppe unter der Leitung des Bundesamts für Justiz, um die Koordination mit den Datenschutzbeauftragten der Kantone sicherzustellen.

7

SCHULUNGEN UND REFERATE

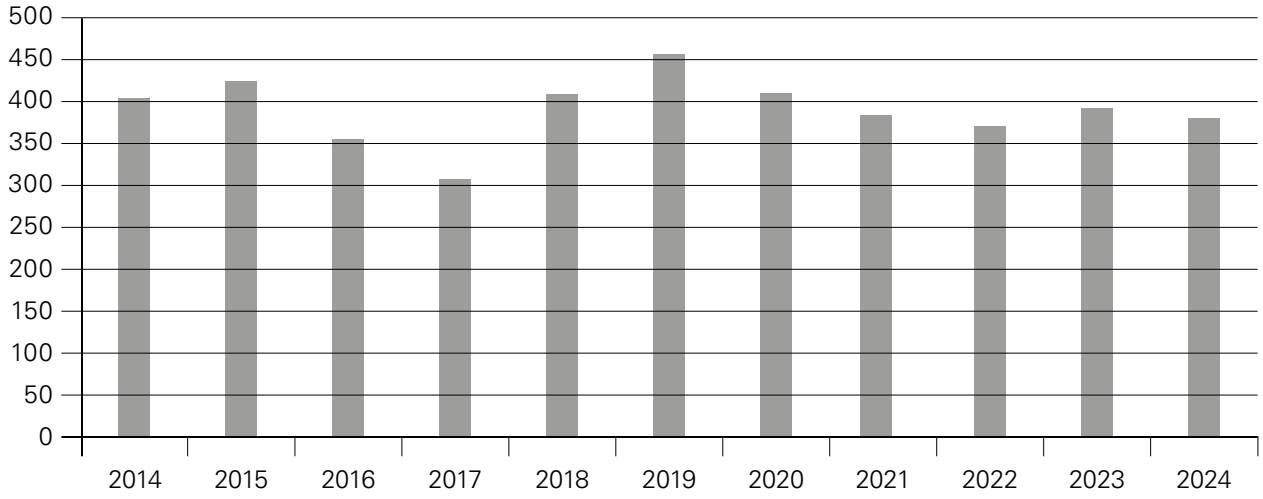
Wie jedes Jahr führte die ASD auch 2024 wieder eine Reihe von Schulungen durch. Neben den jährlich wiederkehrenden Kursen wie jenen des Personalamts zu den Themen Datenschutz und Öffentlichkeitsprinzip sowie den überbetrieblichen Kursen für die Auszubildenden wurde die ASD auch wieder verschiedentlich für interne Weiterbildungen angefragt. Im Berichtsjahr führte die ASD ihre Schulungen für Mitarbeitende im Bereich von «BL Digital+» weiter. Dazu kam eine Veranstaltung für die teilnehmenden des CAS «digitale Transformation». Ferner unterstützte sie die BKSD bei ihren Schulungen, die sie nach der Publikation des Leitfadens «Datenschutz in den Schulen des Kantons Basel-Landschaft» durchführte. Ergänzt wurde dies durch eine Veranstaltung bei der Schulleitungskonferenz.

Die ASD betrachtet Schulungen und Referate nach wie vor als wichtiges Instrument des (digitalen) Datenschutzes. Sie ermöglichen ihr, dem Zielpublikum die Grundsätze des Datenschutzes und der Informationssicherheit nahezubringen. Davon erhofft sie sich ein gesteigertes Bewusstsein für die Bedeutung der Einhaltung der Bestimmungen des IDG. Gerade in Digitalisierungsprojekten ist die frühzeitige Berücksichtigung der Anforderungen von grosser Bedeutung. Solche Schulungen bieten immer auch Gelegenheit für praxisnahe Fragestellungen mit dem entsprechenden Austausch, der auch das gegenseitige Verständnis für den jeweiligen gesetzlichen Auftrag fördert.

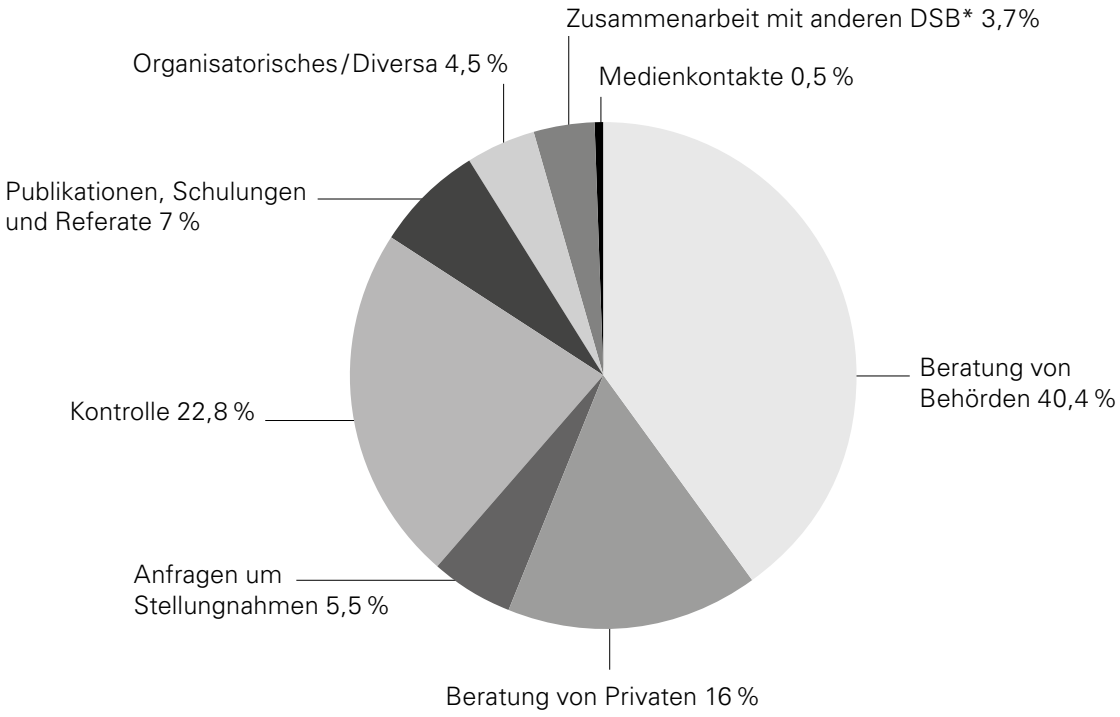
8

ANHANG

ANZAHL NEU ERÖFFNETE GESCHÄFTE



ART DER GESCHÄFTE



(Basis: Anzahl neu eröffnete Geschäfte, Prozentanteile gerundet)

AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragter
Markus Brönnimann

Stv. Datenschutzbeauftragte
Priscilla Dipner-Gerber
Thomas Held

Akademische Mitarbeitende
Ditmar Freitag
Simon Habermacher
Beate Metz
Michael Weschmann

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.

ISSN 2673-6462