

Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2020

Bericht der kantonalen Fachstelle für Datenschutz vom 22. Februar 2021

Inhaltsverzeichnis

Zusammenfassung	2
1 Aufgaben	2
1.1 Vorabkonsultationen	2
1.2 Prüftätigkeit	4
1.3 Rechtsetzung	6
1.4 Einzelanfragen	6
1.4.1 Themen	6
1.4.2 Zahlen	9
1.5 Anzeigen	10
1.6 Register bzw. Verzeichnis	11
1.7 Sensibilisierung	11
1.8 Zusammenarbeit	11
1.9 Geschäftseingänge in Zahlen	11
1.10 Gemeindefachstellen für Datenschutz	13
1.10.1 Arbeitsbesuch	13
1.10.2 Erfahrungsaustausch	13
1.10.3 Übriges	13
2 Personelles und Ressourcen	13
3 Ausblick	14
3.1 Personenregister	14
3.2 Kantonale Einwohnerdatenplattform	14
3.3 Prüfprogramm 2021	14
4 Antrag	14

Zusammenfassung

Im Berichtsjahr bearbeitete die Fachstelle für Datenschutz insgesamt 296 Geschäfte (Vorjahr 251). Vor allem die Einzelanfragen nahmen zu, mehr Zeit beanspruchten auch die Kontrollen.

Ein grosses Thema bei den Einzelanfragen waren Fragen im Zusammenhang mit der Covid-19-Pandemie: vor allem im Schulbereich, etwa zur Durchführung von Prüfungen, der Videoübertragung oder Applikationen zur Unterrichtsunterstützung. Aber auch die Anforderungen an die Einwilligung bei einer Covid-19-Studie oder Homeoffice waren Thema. Daneben war Office 365 einmal mehr von Interesse: Stand bisher der Einsatz im Schulbereich im Vordergrund, stellten sich in diesem Jahr Fragen zur Verwendung in der Verwaltung.

Die Fachstelle für Datenschutz prüfte nebst anderem eDossier, das elektronische Personal-dossier. Die Umsetzung macht einen guten Eindruck. Empfehlungen machte die Fachstelle für Datenschutz zum Wartungsvertrag mit Drittunternehmen und Einpflegen von Dokumenten. Bei der Prüfung des Zutrittsmanagements eines Spitals stellten sich vor allem Fragen zur Aufbewahrungsdauer.

Immer wichtiger werden die Vorabkonsultationen. Eine solche führt die Fachstelle für Datenschutz durch, wenn eine Datenbearbeitung zu einem hohen Risiko für die Grundrechte führt. Themen waren der Einsatz einer Antivirus-Software und einer Webcam auf einer Baustelle sowie das Management von Abwesenheiten. Häufig ging es um die Bearbeitung in der Cloud. Vorabkonsultationen sind meist komplex, interdisziplinär und technisch anspruchsvoll. Sie binden dementsprechend Ressourcen.

Beim Arbeitsbesuch bei einer Gemeindefachstelle war die Unabhängigkeit Thema: Werden andere entgeltliche oder unentgeltliche Tätigkeiten ausgeübt, sollen die Bestimmungen zum Ausstand eng ausgelegt werden. Damit soll den strengen Anforderungen an die Unabhängigkeit der Datenschutzfachstellen Rechnung getragen werden. Zudem dient dies auch der Glaubwürdigkeit und dem Vertrauen.

Herr Präsident
Sehr geehrte Damen und Herren

Die kantonale Fachstelle für Datenschutz (FDS) berichtet dem Kantonsrat nach Art. 36 Abs. 2 des Datenschutzgesetzes (sGS 142.1; abgekürzt DSG) jährlich über ihre Tätigkeit. Der Kantonsrat nimmt vom Bericht Kenntnis. Der Bericht an den Kantonsrat hat dieselbe Stellung wie der Geschäftsbericht der Regierung nach Art. 5a des Staatsverwaltungsgesetzes (sGS 140.1; abgekürzt StVG).¹ Der vorliegende Bericht gibt Rechenschaft über die Tätigkeit der FDS im Jahr 2020.

1 Aufgaben

1.1 Vorabkonsultationen

Art. 8b DSG sieht die Vorabkonsultation vor: Führt eine Datenbearbeitung zu einem hohen Risiko für die Grundrechte der betroffenen Personen, muss das öffentliche Organ dieses Vorhaben der FDS zur Vorabkonsultation vorlegen. Die FDS führte bereits einige Vorabkonsultationen durch. Es handelt sich meist um sehr komplexe und auch technisch anspruchsvolle Vorhaben. Dementsprechend stark beanspruchen sie die Ressourcen. Teilweise wurden nicht alle erforderlichen Unterlagen eingereicht und mussten nachgereicht werden. Immer wieder stellt sich die Frage des

¹ Vgl. Botschaft und Entwurf der Regierung zum Datenschutzgesetz vom 20. Mai 2008: Bemerkungen zu Art. 36 Abs. 3 des Entwurfs (ABI 2008, 2299 ff., 2329).

Zeitpunkts der Einreichung: Die Vorabkonsultation ist meist eine Folge der Datenschutz-Folgenabschätzung (Art. 8a DSGVO). Diese muss vorgängig einer Datenbearbeitung, die zu einem hohen Risiko für die Grundrechte führen kann, gemacht werden. Demzufolge muss auch die Vorabkonsultation jeweils vor der entsprechenden Datenbearbeitung erfolgen. Nicht zuletzt deshalb, weil andernfalls hohe Aufwendungen und Kosten entstehen können, wenn ein Vorhaben datenschutzrechtliche Mängel aufweist. Erarbeitet das öffentliche Organ eine Datenschutz-Folgenabschätzung oder befasst es sich mit der Vorabkonsultation, ist dies nicht (nur) eine lästige Pflicht, sondern zeichnet das moderne und verantwortungsbewusste öffentliche Organ aus, das mit sehr vielen sensiblen Daten der Bürgerinnen und Bürger sorgfältig umzugehen weiss. Dies schafft Vertrauen.

Zunehmen dürften Vorabkonsultationen, die mehrere kantonale Datenschutzstellen gemeinsam durchführen; dies deshalb, weil die Kantone immer häufiger gleiche Applikationen einsetzen. Ein Beispiel dafür ist die Swiss Library Service Platform (SLSP) der Universität St.Gallen. Ein sehr häufiges Thema bei den Vorabkonsultationen ist die Datenbearbeitung in einer Cloud, wie die folgenden Beispiele zeigen:

– *Antivirus-Software*

Ein öffentliches Organ beabsichtigte, eine neue Antivirus-Software eines US-Unternehmens einzusetzen. Es handelt sich um eine Software der «neuen Generation»: Sie basiert nicht ausschliesslich auf einem signaturbasierten Verfahren, sondern setzt auf künstliche Intelligenz und maschinelles Lernen. Wie bereits im Tätigkeitsbericht 2019 (32.20.03) dargelegt, dürfen besonders schützenswerte Personendaten und solche, die einem Berufs- oder speziellen Amtsgeheimnis unterliegen, nicht in einer US-Cloud bearbeitet werden. Des Weiteren müssen folgende Voraussetzungen erfüllt sein: Es darf kein gleichwertiges Produkt eines Anbieters in einem Land mit angemessenem Datenschutzniveau gemäss Staatenliste² des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) verfügbar sein. Es muss Schweizer Recht gelten und der Gerichtsstand in der Schweiz sein. Zudem muss das öffentliche Organ mit dem US-Unternehmen einen Vertrag – die Allgemeinen Geschäftsbedingungen (AGB) genügen nicht – abschliessen, der ein angemessenes Datenschutzniveau gemäss Staatenliste gewährleistet. Das angemessene Datenschutzniveau gilt auch für den Serverstandort. Weitere Empfehlungen betrafen die Zugriffsrechte, die Zweckmässigkeit und die Aufbewahrungsdauer.

– *CAREMAcare im Spital*

Vorgesetzte in einem Spital verwenden für das Management von Abwesenheiten eine Applikation. Diese soll durch das Nachfolgemodul CAREMAcare ersetzt und künftig in der Cloud bearbeitet werden. Hauptfrage war, unter welchen Voraussetzungen die Auslagerung des Absenzenmanagements in die Cloud zulässig ist. Da es sich bei den zu bearbeitenden Daten um besonders schützenswerte Personendaten handelt, gelten erhöhte Anforderungen an die Sicherheit. Dazu gehört z.B. – wegen des Cloud Act³ – dass Applikationen gewählt werden, die keinen Bezug zu den USA haben. Ein weiteres Augenmerk wurde auf die Zugriffe gelegt. Diese dürfen von ausserhalb der Organisation nur über das interne Netzwerk und nur innerhalb der Schweiz erfolgen.

– *Moodle*

Eine Berufsfachschule plante, das Hosting von Moodle an einen privaten Dritten auszulagern. Moodle ist ein Kursmanagementsystem und eine Lernplattform. Bei einem solchen Vorhaben sind wichtige Fragen, wo sich der Sitz des beauftragten Unternehmens und die Server befinden. Die Prüfung der Vereinbarung zeigte, dass sich der Serverstandort in Gais, Appenzell Ausserrhoden, befindet. Damit werden die datenschutzrechtlichen Anforderungen erfüllt.

² Siehe www.edoeb.admin.ch > Datenschutz > Handel und Wirtschaft > Übermittlung ins Ausland > Staatenliste.

³ Vgl. Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2019, S. 4 f (32.20.03).

– *Swiss Library Service Platform an der Hochschule*

Die bisherigen Hochschulbibliothekskataloge werden neu in der Swiss Library Service Platform (SLSP) in einem gesamtschweizerischen Bibliothekssystem geführt. Damit können alle Nutzenden mit einem einzigen Bibliothekskonto auf die Kataloge aller angeschlossenen Hochschulbibliotheken in der Schweiz zugreifen und von jeder Bibliothek Medien ausleihen. Einige Verträge, Entwürfe und Konzepte prüften bereits die Datenschutzfachstellen der Kantone Basel-Stadt, Bern und Zürich. Die FDS prüfte die Übereinstimmung mit dem DSG. Sie empfahl u.a., den Vertrag zwischen dem öffentlichen Organ und der Anbieterin anzupassen, so dass für die Weiterübertragung der Datenbearbeitung die schriftliche Zustimmung des auftraggebenden öffentlichen Organs im Voraus einzuholen ist. Weiter fehlten im Vertrag Vereinbarungen über Konventionalstrafe oder Strafbestimmungen des DSG. Zudem musste eine fehlende Benutzungsordnung einer der teilnehmenden Hochschulen erstellt werden.

– *Webcam bei einer Baustelle*

Bei der Baustelle eines öffentlichen Organs ist eine Webcam installiert. Die Webcam dient dazu, den Baufortschritt auf der Baustelle zu zeigen, die Donatorinnen und Donatoren zu informieren und die Webseite für Besucherinnen und Besucher attraktiver zu machen. Bei einer Webcam handelt es sich um eine Videokamera, die in gewissen Zeitabständen oder auf Anfrage der Benutzenden Live-Bilder liefert. Allgemein dienen Webcams der Unterhaltung und sollen die entsprechenden Webseiten für die Besucherinnen und Besucher attraktiver machen.⁴

Im vorliegenden Fall werden teilweise Personendaten bearbeitet: Personen können nicht nur anhand des Gesichts, sondern auch anhand ihrer Kleidung, mitgeführter Gegenstände oder Hunde bestimmt werden. Fussgängerinnen und Fussgänger oder Fahrzeuge können der Aufnahme nicht ausweichen. Für die Veröffentlichung braucht es eine Rechtsgrundlage. Eine solche ist nicht vorhanden. Deshalb dürfen Personen und Fahrzeuge nicht erkennbar sein, auch nicht aufgrund besonderer Merkmale. Weiter empfahl die FDS den Bildausschnitt auf die Baustelle und die Aufnahmen auf die Arbeitszeit auf der Baustelle zu beschränken. Dies genügt für den Zweck, den Baufortschritt zu zeigen. Mit dem externen Unternehmen, das die Webcam betreibt, müssen die datenschutzrechtlichen Vorgaben schriftlich in einer Vereinbarung geregelt werden. Weiter zu beachten waren die Vorgaben zur Informationssicherheit und die Pflicht zur Datenschutz-Folgenabschätzung und Vorabkonsultation.

– *Infosearch bei der Kantonspolizei St.Gallen*

Die Kantonspolizei St.Gallen beabsichtigt die Einführung von Infosearch. Dabei handelt es sich um eine polizeiliche Fachapplikation, welche die Dokumentation und Verwaltung von verdeckt erhobenen Informationen unterstützt. Die Informationen werden in Zusammenarbeit mit vertraulichen Quellen sowie anlässlich von Einsätzen mit verdeckt ermittelnden Polizistinnen und Polizisten erhoben. Da die Applikation die Verknüpfung verschiedener Daten und Bearbeitungsmöglichkeiten erlaubt, empfahl die FDS betreffend deren Verwendung eine Rechtsgrundlage auf Verordnungsstufe anzustreben.

1.2 Prüftätigkeit

eDossier

Auf Wunsch des Lenkungsausschusses prüfte die FDS zusammen mit dem Dienst für Informatikplanung (DIP) das eDossier. Ab dem Jahr 2018 wurde das papierene Personaldossier schrittweise durch das elektronische Dossier abgelöst. Die Applikation ist in SAP HR integriert und wird mit Unterstützung eines Drittunternehmens betrieben. Besprochen wurden u.a. das Abrufverfah-

⁴ Siehe www.edoeb.admin.ch > Datenschutz > Technologien > Videoüberwachung > Webcams.

ren, die Vereinbarung mit dem Drittunternehmen, die Erfassung der Personendaten, Authentisierung und Berechtigungen, Klassifizierung und Massnahmen sowie die Aufbewahrungsdauer von Dossiers, die dem Staatsarchiv abgeliefert werden.

Die Umsetzung des Projekts macht hinsichtlich Datenschutz und Informationssicherheit einen guten Eindruck. Empfehlungen wurden bezüglich des Wartungsvertrags mit dem Drittunternehmen gemacht: Integrierender Bestandteil des Wartungsvertrags war eine nicht aktuelle Version der AGB der Schweizerischen Informatikkonferenz (SIK). Verschiedene datenschutzrechtliche Anforderungen wie die Gewährleistung der technischen und organisatorischen Massnahmen, die Meldung einer Datenschutzverletzung⁵, das Kontrollrecht oder der Umgang mit den Personendaten bei Vertragsbeendigung sind darin nicht geregelt. Deshalb muss die aktuellste Version der AGB SIK integrierender Bestandteil des Wartungsvertrags sein. Des Weiteren muss beim Einpflegen von Dokumenten zwingend das Vier-Augen-Prinzip gelten: Falsch hinterlegte Dossiers bzw. Dokumente können zu einem schweren Eingriff in die Persönlichkeitsrechte der betroffenen Mitarbeitenden führen.

Das Abrufverfahren – darum handelt es sich bei eDossier – als solches muss nicht separat geregelt werden: Jede Datenbekanntgabe braucht eine genügende Rechtsgrundlage. Die FDS vertritt die Ansicht, dass eine Bestimmung, welche die Datenbekanntgabe genügend bestimmt in einem formellen Gesetz regelt, ausreicht. Müsste das Abrufverfahren in jedem Fall zusätzlich zu den Voraussetzungen für eine Datenbekanntgabe geregelt werden, hätte dies zur Konsequenz, dass etliche Erlasse revidiert werden müssten. Dies, ohne dass damit ein wesentlicher Mehrwert im Sinn des Datenschutzes verbunden wäre. Im digitalen Zeitalter scheint es überholt, das Abrufverfahren als solches zu regeln.

Applikation Dorian beim Baudepartement

Im Jahr 2019 prüfte die FDS zusammen mit dem DIP die Fachapplikation Dorian. Die Prüfung wurde im Frühling 2020 abgeschlossen. Dorian beinhaltet unter anderem nicht anonymisierte Entscheide, Rechtsauskünfte, Urteile und Verfügungen. Es handelt sich um eine Wissensdatenbank, die einem effizienten Wissensmanagement und der einheitlichen Rechtsprechung dient. Es geht darum, sich zu informieren, wie in vergleichbaren Fällen entschieden wurde. Sie dient hingegen nicht der Fallbearbeitung. Für diesen Zweck braucht es keine Personendaten. Die FDS vertrat deshalb die Auffassung, dass die Entscheide in Dorian zu anonymisieren seien. Da dies gemäss Baudepartement wegen des Umfangs und der Tatsache, dass der Name das Suchkriterium bildet, nicht möglich war, ist es notwendig, für Dorian eine Rechtsgrundlage zu schaffen. Zudem dürfen in Dorian nur nicht besonders schützenswerte Personendaten bearbeitet und muss der Zugriff auf Stellen innerhalb des Departementes beschränkt werden. Es gelten dieselben Aufbewahrungsfristen wie für die – nicht in Dorian bearbeiteten – Fallakten.

Zutrittsmanagement Spital

Ein Spital führte im Jahr 2020 ein neues Schliesssystem ein. Die Zutritte in die Räumlichkeiten sind personalisiert, d.h. mit der geeigneten Hard- und Software ist ersichtlich, wann welche Person den Schlüssel wo genutzt hat und ob sie Zutritt erhalten hat oder nicht. Die FDS prüfte, ob die datenschutzrechtlichen Bestimmungen eingehalten werden. Hauptthema war die Aufbewahrungsdauer der Personendaten: Daten der Projektphase müssen gelöscht werden, sobald sie nicht mehr benötigt werden. Buchungs- und Bewegungsdaten müssen nach drei Monaten gelöscht werden. Werden sie länger aufbewahrt, etwa zu statistischen Zwecken oder zur Nachvollziehbarkeit bei Soft- und Hardwarefehlern, müssen sie anonymisiert werden, denn für diese Zwecke braucht es keine Personendaten. Zudem handelt es sich bei den Bewegungsdaten um sensible Daten.

⁵ Art. 9a Abs. 3 DSG.

Schengen-Kontrolle beim Migrationsamt

Für die Schengen-Kontrolle wurden erste Vorarbeiten getätigt. Aus Ressourcengründen konnte sie aber noch nicht durchgeführt werden. Sie wird im Jahr 2021 nachgeholt. Die Koordinationsgruppe der Schweizerischen Datenschutzbeauftragten empfiehlt im Leitfaden für die Kontrolle der Nutzung des Schengener Informationssystems alle zwei Jahre eine Prüfung. Die FDS hat im Jahr 2019 eine Schengen-Kontrolle bei der Kantonspolizei durchgeführt. Damit liegt sie im Plan.

Applikation Jagd und Fischerei

Die zuständige Stelle bat aus personellen Gründen bzw. Ressourcengründen um eine Verschiebung der Prüfung. Die Prüfung findet im Frühling 2021 statt.

1.3 Rechtsetzung

Digitaler Posteingang

Die Staatskanzlei beabsichtigte, die «digitale Postbearbeitung» einzuführen: Die eingehenden postalischen Sendungen sollten zentral digitalisiert werden. Dafür wurde eine Dienstanweisung erlassen. Ein wichtiger Punkt war die Aufbewahrung der physischen Post: Bis die physischen Schreiben vernichtet werden, müssen diese sicher vor dem Zugriff unberechtigter Dritter aufbewahrt werden. Weitere Anregungen machte die FDS bei der klaren Regelung der Kompetenzen und der Sensibilisierung. Insgesamt machte die Umsetzung in datenschutzrechtlicher Hinsicht einen guten Eindruck.

Im Weiteren hat die FDS zu folgenden Erlassentwürfen und Vorhaben Stellung genommen:

- Schengen-Follow-up;
- Gesetz über den Allgemeinen Teil der Abgabenerhebung und die Kontrolle des grenzüberschreitenden Waren- und Personenverkehrs durch das Bundesamt für Zoll und Grenzsicherheit sowie Totalrevision des Zollgesetzes zum neuen Zollabgabengesetz;
- Verordnung über Kurse und Prüfungen in Lebensmittelhygiene und Suchtprävention (sGS 553.12).

1.4 Einzelanfragen

1.4.1 Themen

Im Berichtsjahr beschäftigte die FDS – wie auch bei den Vorabkonsultationen – das Thema Cloud, insbesondere die Vereinbarungen mit Drittunternehmen. Dabei zeigt sich die erfreuliche Entwicklung, dass datenschutzrechtliche Aspekte heute meist geregelt werden. Früher war dies häufig nicht der Fall. Damals standen Kosten und andere Konditionen im Vordergrund. Datenschutzrechtliche Belange zu regeln ist nicht nur aufgrund des DSG zwingend, sondern auch aufgrund der Tatsache, dass eine Datenbearbeitung in der Cloud häufig ein wesentlich höheres Risiko darstellt, als wenn die Datenbearbeitung «on premise»⁶ stattfindet. Die Datenbearbeitung in einer (öffentlichen) Cloud erscheint auf den ersten Blick häufig attraktiv, verspricht sie doch Kosten- und Effizienzgewinne. Dabei geraten die möglichen Folgekosten schnell aus dem Blickfeld: Das öffentliche Organ bleibt auch in der Cloud, wo die Kontrollmöglichkeiten häufig klein sind, für die Datenbearbeitung verantwortlich. Wird gegen Datenschutzbestimmungen verstossen, können sich hohe Kosten oder Reputationsschäden ergeben.

Ein zweites wichtiges Thema war die Covid-19-Pandemie. Die FDS bearbeitete zahlreiche Anfragen insbesondere aus dem Schulbereich. Die Covid-19-Pandemie hat Auswirkungen auf das Grundrecht auf Privatsphäre: Eilig eingeführte digitale Lösungen, um Schulunterricht oder Ar-

⁶ In den eigenen Räumlichkeiten, vor Ort oder lokal.

beitsleben trotz Lockdown aufrechterhalten zu können, entsprachen wohl nicht immer dem bisherigen Standard. Es ist nachvollziehbar, dass in einer derart ausserordentlichen Situation andere Massstäbe angesetzt werden, die Verhältnismässigkeit bemisst sich auch nach den Umständen. Die Grundrechte gelten gleichwohl auch in einer ausserordentlichen Situation. Wichtig ist zu berücksichtigen, dass nach Ende der Covid-19-Pandemie die Grundrechtseinschränkungen nicht gleich gross sein können, wie während der Covid-19-Pandemie; d.h., Anwendungen etwa im Schulbereich, die nicht vollumfänglich datenschutzkonform sind, müssen durch solche ersetzt werden, die den Datenschutzerfordernissen vollumfänglich genügen.

Allgemein stellt die FDS fest, dass der Grundsatz der Verhältnismässigkeit oft zu wenig beachtet wird: Damit ein Eingriff in das Grundrecht der Privatsphäre rechtmässig ist, muss nicht nur die rechtliche Grundlage vorhanden, sondern der Eingriff auch verhältnismässig sein. So ist z.B. die Onlineabfrage über Eigentümerinnen und Eigentümer, wie dies in vielen Gemeinden möglich ist, nicht mit einer elektronischen Anfrage im Einzelfall (z.B. E-Mail) vergleichbar. Onlineabfragen sind wesentlich einfacher und schneller zu handhaben, was der Effizienz dienen kann. Die Gefahr für schwerwiegendere Eingriffe in die Persönlichkeitsrechte ist aber grösser. Auch wenn keine Serienabfragen möglich sind, sind in kürzerer Zeit viel mehr Daten verfügbar. Ob eine Massnahme erforderlich ist, muss allgemein sorgfältig geprüft werden, ebenso müssen die öffentlichen und die betroffenen privaten Interessen sehr sorgfältig gegeneinander abgewogen werden.

Nachfolgend werden einzelne Fälle zu diesen Themen und weitere allgemein interessierende Anfragen zusammengefasst:

Covid-19-Pandemie – Durchführung von Prüfungen

Es stellte sich die Frage, ob es zulässig sei, Prüfungen online mit einem Monitoring durch Video- und Audioüberwachung durchzuführen. Die Prüfungsergebnisse wurden auf dem Server der Bildungseinrichtung, die jeweilige Prüfungsumgebung hingegen auf US-Servern gespeichert. Die Studierenden konnten eine Probeprüfung absolvieren und es wurde über das Vorgehen informiert. Die Studierenden konnten freiwillig entscheiden, ob sie die Prüfungen online oder zu einem späteren Zeitpunkt absolvieren möchten. Aus Sicht der FDS ist die Speicherung der Daten in den USA nicht angemessen. Auch ist nicht ersichtlich, weshalb bei den schriftlichen Prüfungen Aufnahmen notwendig sind. Bei den mündlichen Prüfungen ist zu differenzieren: Aus Gründen der Beweiskraft in einem allfälligen Rechtsmittelverfahren kann dafür eine Notwendigkeit gegeben sein. Dafür genügt aber eine Tonaufnahme, eine Videoaufnahme der Studierenden ist dafür nicht erforderlich.

Covid-19-Pandemie – Videoübertragung und Applikationen zur Unterrichtsunterstützung

Aufgrund des coronabedingten Lockdowns im Frühjahr waren im Bildungsbereich einerseits Applikationen und Software für Videokonferenz bzw. Videoübertragung Thema, andererseits webbasierte Applikationen zur Unterrichtsförderung und -unterstützung. Die Applikationen für Videokonferenzen waren teilweise nicht darauf ausgerichtet, Unterrichtszwecken zu dienen. Deshalb musste geprüft werden, was mit allfälligen Schülerdaten, die für das Login notwendig waren (z.B. Mailadresse) geschieht.

Bei den webbasierten Applikationen zur Unterrichtsförderung und -unterstützung stellte sich einmal mehr die Problematik der Cloud-Dienste. Dabei muss in jedem einzelnen Fall eine Risikoabwägung stattfinden.

Covid-19-Pandemie – Corona-Studie

Im Zusammenhang mit einer Studie zur Immunität stellte sich die Frage, ob eine elektronische Einwilligung aus datenschutzrechtlicher Sicht genüge. Des Weiteren war vorgesehen, dass ein ausländisches Unternehmen mit der Analyse von Symptomdaten beauftragt wird.

Nach Ansicht der FDS genügt die elektronische Einwilligung im vorliegenden Fall, zumal das öffentliche Organ für die Einhaltung der Datenschutzbestimmungen beweispflichtig ist. Die Einwilligungserklärung muss aber erhöhte Anforderungen erfüllen, es muss z.B. sichergestellt werden, dass die einwilligende Person Kenntnis hat, wo die Proben aufbewahrt werden und an wen sie bekanntgegeben werden sollen. Zudem muss die Einwilligung jederzeit widerrufen werden können. Wie bereits oben erwähnt, sollen besonders schützenswerte Personendaten nicht auf einem Server eines Unternehmens gespeichert werden, dessen Datenschutzniveau gemäss Staatenliste nicht angemessen ist.

Covid-19-Pandemie – Homeoffice

Während des Lockdowns war Homeoffice immer wieder Thema. Auch wenn die Stelle sensible Personendaten bearbeitet, wie dies bei öffentlichen Organen häufig der Fall ist, spricht grundsätzlich nichts gegen Homeoffice, sofern einige Voraussetzungen beachtet werden. Zu beachten sind die organisatorischen und technischen Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten. Z.B. muss eine Zugriffsbeschränkung eingerichtet und der Speicher verschlüsselt werden. Für die Arbeit zu Hause darf in der Regel nur ein kantonseigenes Notebook verwendet werden. Die Speicherung ist ausschliesslich in den dafür vorgesehenen Geschäftsablagen zulässig. Papierakten sollen zu Hause nur dann bearbeitet werden, wenn es zwingend und nicht anders handhabbar ist. Entsprechend sorgfältig muss der Transport sein.

Covid-19-Pandemie – Liste mit erkrankten Mitarbeitenden veröffentlichen

Darf eine vorgesetzte Person eine Liste erkrankter Mitarbeitender führen und im Amt bzw. der Abteilung veröffentlichen? Bei Angaben zum Gesundheitszustand handelt es sich einerseits um besonders schützenswerte Personendaten. Andererseits hat der Arbeitgeber eine Fürsorgepflicht. Zudem wird das öffentliche Gut «Gesundheit» während der Covid-19-Pandemie sehr stark gewichtet, sowohl zum Schutz der eigenen Gesundheit als auch zum Schutz der Gesellschaft. Um diesen Schutz gewährleisten zu können, darf die vorgesetzte Person eine Liste erstellen, aus der ersichtlich ist, welche Mitarbeitenden sich mit dem Virus angesteckt haben. Diese Liste dient aber nur der vorgesetzten Person, welche die betroffenen Mitarbeitenden sofern erforderlich informiert. Die Liste muss sich zudem auf die aktuellen Ereignisse beschränken und ist zu vernichten, sobald der Grund für das Führen dieser Liste weggefallen ist.

Office 365

Die Verwendung von Office 365 an *Schulen* war bereits im Jahr 2018 Thema⁷. Eine rechtskonforme Nutzung setzt die Unterzeichnung einer Zusatzvereinbarung voraus, die bestimmt, dass Schweizer Recht und Gerichtsstand in der Schweiz gelten. Zudem dürfen keine besonders schützenswerten Personendaten oder solche, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen, bearbeitet werden. Faktisch geht es um die Bearbeitung schulischer Belange, z.B. von Aufgabenblättern. Im Berichtsjahr stellte sich die Frage der Verwendung von Office 365 im Bereich der *Verwaltung*. Seit Herbst 2020 gibt es eine mit dem Schulbereich vergleichbare Zusatzvereinbarung. Da im Verwaltungsbereich viele sensible Daten bearbeitet werden, gilt es zusätzliche Punkte zu beachten: Das öffentliche Organ muss ein durchsetzbares Kontrollrecht für eine datenschutzrechtliche Prüfung erhalten, es muss der Weiterübertragung der Datenbearbeitung an einen Dritten vorgängig zustimmen und das Drittunternehmen darf die Personendaten nur für die Auftragserfüllung für das öffentliche Organ verwenden. Wie bei allen Cloud-Anwendungen muss vorgängig eine Risikoanalyse im Einzelfall gemacht werden.

⁷ Vgl. Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2019, S. 4 (32.20.03).

Datenbekanntgabe für statistische Zwecke

Zur Diskussion stand die Bekanntgabe der nicht anonymisierten Versichertennummer an die Fachstelle für Statistik. Die gesetzliche Grundlage für die Bekanntgabe war zwar vorhanden. Da es sich bei einer Datenbearbeitung um einen Eingriff in ein Grundrecht handelt, muss neben der gesetzlichen Grundlage die Verhältnismässigkeit gegeben sein. Die Prüfung hat ergeben, dass es im konkreten Fall die nicht anonymisierten Versichertennummern zur Aufgabenerfüllung nicht braucht. Somit müssen die Daten vor der Bekanntgabe anonymisiert werden.

Mediananfragen

Bei den Medienanfragen waren die Auslagerung des Contact Tracing an Private und die Frage der Gesichtserkennungssoftware bei der Kantonspolizei Thema. In den anderen Fällen ging es um eine Videoüberwachung an einer Schule, die Datensammlung durch einen Privaten und die Anpassung der AGB. In letzteren Fällen war nicht die FDS zuständig.

1.4.2 Zahlen

Im Jahr 2020 bearbeitete die FDS 264 Einzelanfragen (Vorjahr 217), fast ein Fünftel mehr als im Vorjahr. Wie bereits in den Vorjahren ist schwierig zu eruieren, was die Gründe dafür sind – die gehäuften Fragen im Zusammenhang mit der Covid-19-Pandemie dürften aber eine Rolle spielen. Bei Zuständigkeit, Herkunft und zeitlichem Aufwand ergaben sich gegenüber dem Vorjahr keine wesentlichen Änderungen.

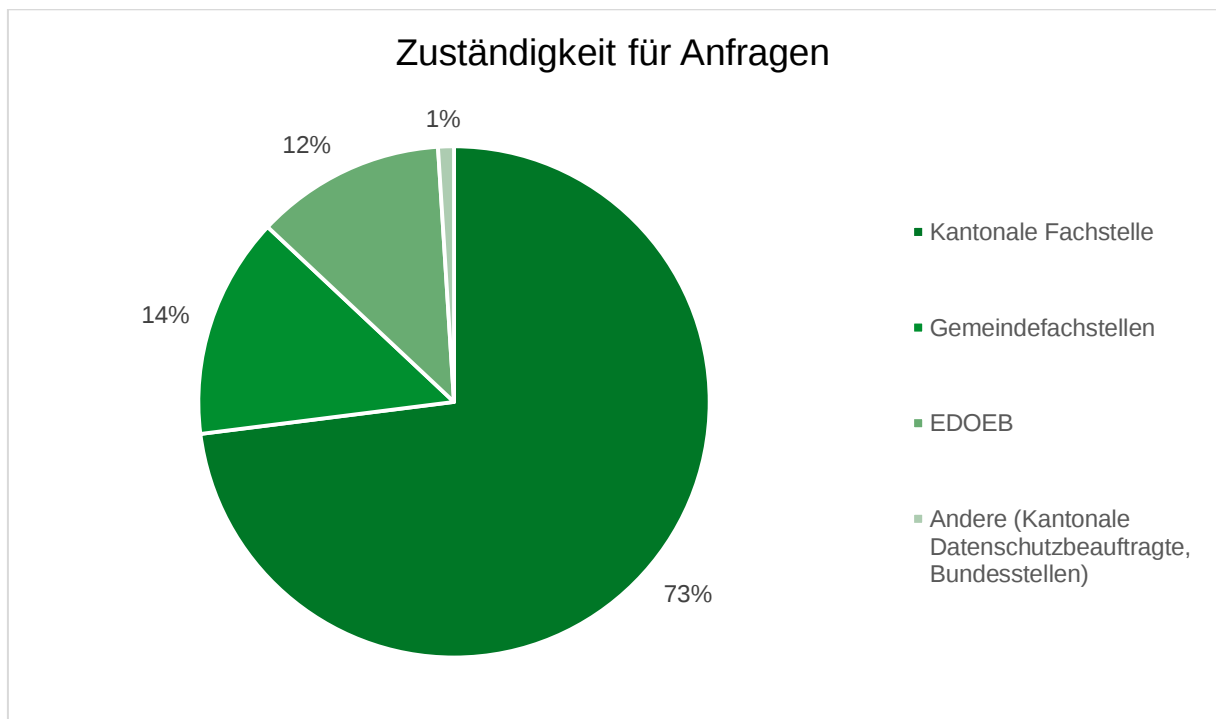


Abbildung 1: Zuständigkeit für Einzelanfragen in Prozent im Jahr 2020.

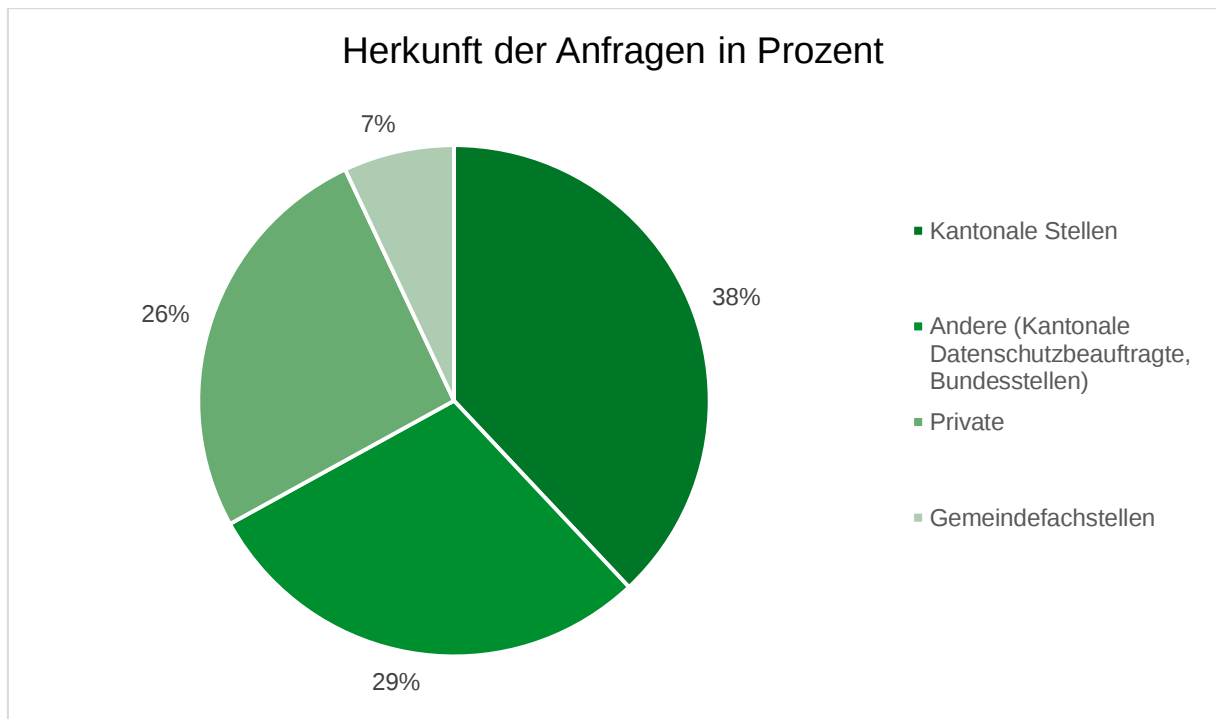


Abbildung 2: Herkunft der Einzelanfragen in Prozent im Jahr 2020.

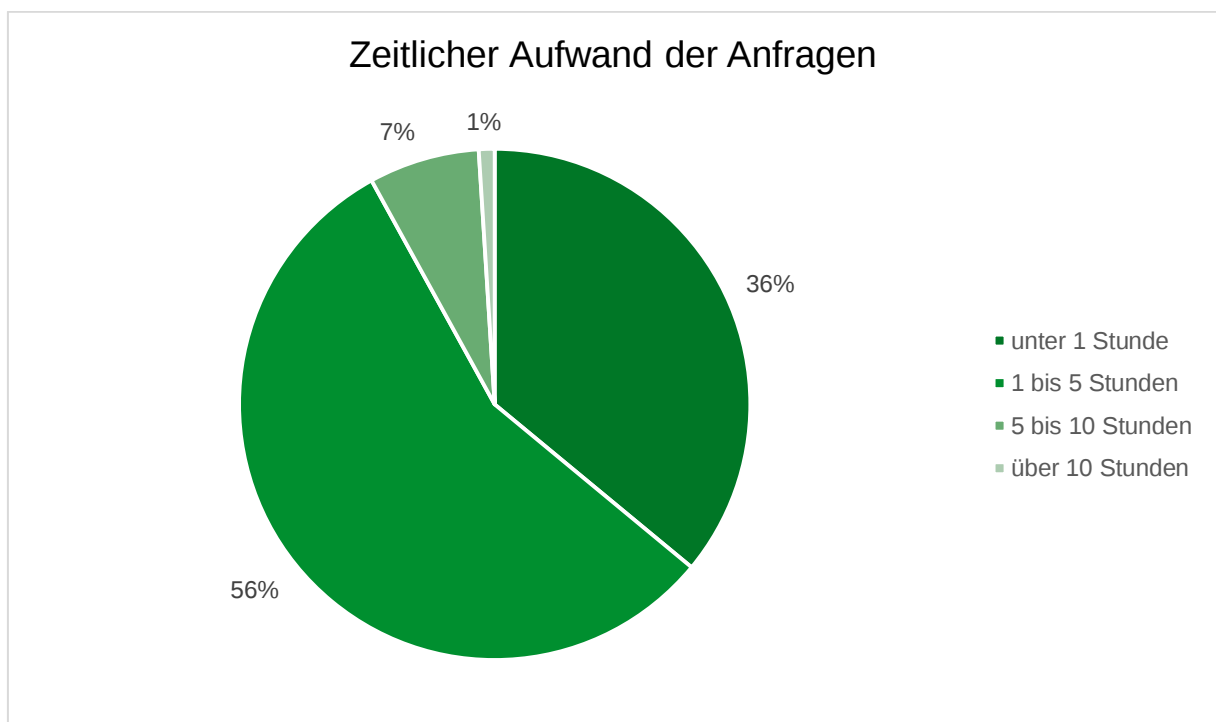


Abbildung 3: Bearbeitungsaufwand von Einzelanfragen in Prozent im Jahr 2020.

1.5 Anzeigen

Im Jahr 2020 ging bei der FDS keine Anzeige ein.

1.6 Register bzw. Verzeichnis

Die wenigen Anfragen der öffentlichen Organe zum Register der Datensammlungen waren mehrheitlich praktischer oder organisatorischer Natur. Bei der FDS wurde kein Einsichtsgesuch gestellt.

Das revidierte DSG verpflichtet die Justizbehörden und die Polizei ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen. Gleichzeitig wurden die Bestimmungen zum Register der Datensammlungen beibehalten. Faktisch bedeutet dies, dass diese Behörden zwei Verzeichnisse führen müssen, die inhaltlich teilweise deckungsgleich sind. Für Verwirrung sorgte die Abgrenzung, die Konsequenzen hat: Das Register der Datensammlungen ist öffentlich, das Bearbeitungsverzeichnis muss lediglich der FDS gemeldet werden. Der administrative Aufwand für die Führung zweier Register ist gross, der Mehrwert hingegen, zumal der Inhalt teilweise gleich ist, klein. Die verpflichteten Organe ergänzten daher ihr Register um diejenigen Angaben, die das Verzeichnis der Bearbeitungstätigkeiten erfordert, z.B. über die Aufbewahrungsdauer oder die beauftragten Dritten und stellte es der FDS zu. Eine einheitliche Pflicht zur Führung eines Verzeichnisses bzw. Registers wäre zu begrüssen.

1.7 Sensibilisierung

Die FDS sensibilisierte mit einer Broschüre die IT-Fachleute des Kantons. Wie in jedem Jahr arbeitete die FDS zudem beim E-Learning Informationssicherheit und Datenschutz mit. Nach wie vor sind Merkblätter und Checklisten wichtig. Die FDS hat insbesondere die Merkblätter über die neuen Instrumente regelmässig überarbeitet.

1.8 Zusammenarbeit

Aufgrund der Covid-19-Pandemie fand im Berichtsjahr keine Versammlung von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, statt. Der Austausch mit anderen kantonalen Datenschutzbeauftragten fand aber im Rahmen der Mitarbeit im Vorstand von privatim statt. Themen waren der Einsatz von Office 365 in Verwaltungen, Stellungnahmen zu verschiedenen Vernehmlassungen und Cloud. Auch bearbeitete die FDS einige Anfragen anderer kantonomer Datenschutzbeauftragter. Daneben pflegte die FDS wie bisher den Austausch mit zahlreichen Stellen des Kantons und mit den Gemeindefachstellen für Datenschutz und insbesondere mit dem DIP.

1.9 Geschäftseingänge in Zahlen

Im Berichtsjahr gingen bei der FDS 296 Geschäfte ein (Vorjahr 251). Damit zeigt sich eine Kontinuität seit Beginn: Tendenziell nehmen die Geschäftseingänge zu, zwischendurch gibt es immer wieder Jahre mit tieferen Geschäftseingängen.

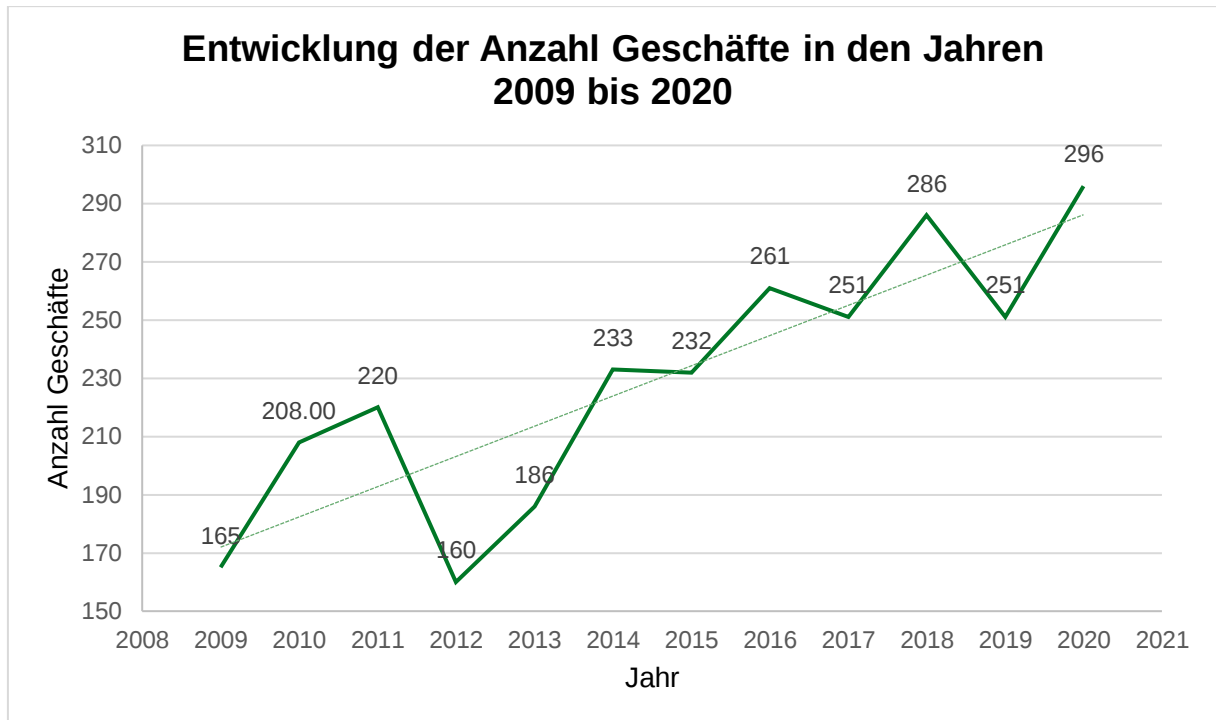


Abbildung 4: Entwicklung der Geschäftszahlen in den Jahren 2009 bis 2020.

Gegenüber dem Vorjahr wendete die FDS mehr Zeit für die Bearbeitung der Einzelanfragen auf und etwas mehr Zeit für die Kontrollen. Die übrigen Zahlen bewegen sich im Rahmen des Vorjahres.

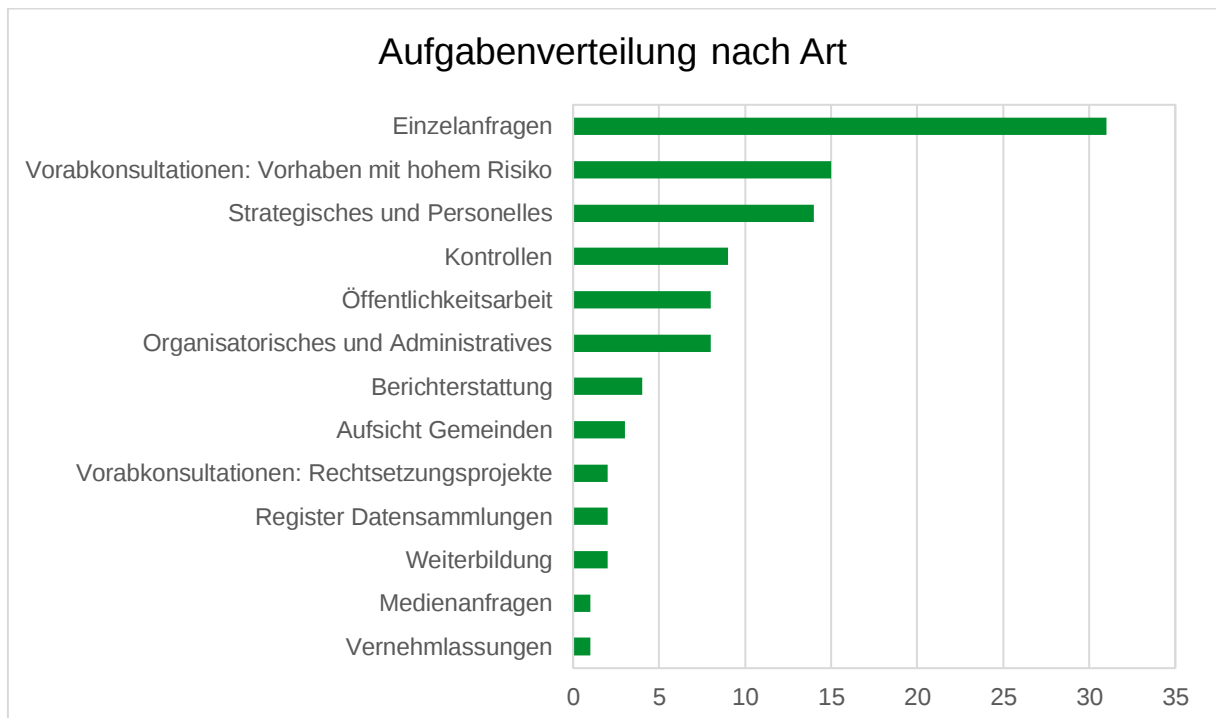


Abbildung 5: Aufgabenverteilung gemäss interner Arbeitszeiterfassung in Prozent (gerundet) im Jahr 2020.

1.10 Gemeindefachstellen für Datenschutz

1.10.1 Arbeitsbesuch

Die FDS machte zusammen mit dem DIP einen Arbeitsbesuch bei der Gemeindefachstelle Rheintal/Werdenberg/Sarganserland. FDS und DIP erörterten mit der Fachstellenleitung folgende Themen: Ausgestaltung der Stelle, Infrastruktur einschliesslich Informatik, Unabhängigkeit, Aufgabenerfüllung und Zusammenarbeit. Der Fachstellenleiter ist von der Stadt Buchs gewählt. Seit Anfang 2020 erfüllt seine Mitarbeiterin die Aufgaben gemäss DSG. Die Gemeindefachstelle macht einen guten Eindruck: Die Mitarbeiterin nimmt ihre Aufgabe aktiv, offen und engagiert wahr. Sie führt regelmässig Kontrollen durch. Das ist erfreulich, da dies bisher nicht systematisch gemacht wurde. Ebenfalls besprochen wurde die Unabhängigkeit: Der Leiter der Fachstelle ist seit der Amtsdauer 2020/2024 Mitglied des Kantonsrates. Die Mitarbeiterin ist Präsidentin eines Vereins, mit dem eine Vereinbarungsgemeinde einen Leistungsauftrag hat. In beiden Fällen ist keine Unvereinbarkeit ersichtlich. Unvereinbarkeit heisst, dass ein Verbot existiert, gleichzeitig einer anderen Behörde anzugehören. Kommt es inskünftig im Einzelfall zu einer Interessenkollision, sind die Ausstandsgründe zu beachten. Sofern Ermessen besteht, sollen die Bestimmungen zum Ausstand eng ausgelegt werden, damit kein Anschein von Befangenheit entsteht und den strengen Anforderungen an die Unabhängigkeit der Datenschutzfachstellen Genüge getan wird. Dies dient der Stärkung sowohl der Unabhängigkeit als auch der Glaubwürdigkeit und des Vertrauens. Weiter machte die FDS Anregungen zum Zugriffsschutz und zum Internetauftritt.

1.10.2 Erfahrungsaustausch

Thema des Erfahrungsaustausches mit den Gemeindefachstellen waren die Bewirtschaftung der Daten und der Zugriff auf Daten in der kantonalen Einwohnerdatenplattform. Besprochen wurde zudem die Zusammenarbeit der Datenschutz-Fachstellen bei der Datenaustauschvereinbarung im Rahmen von E-Government. Weitere Themen waren das Krebsregister, Office 365 und das Backup in einer US-Cloud.

1.10.3 Übriges

Die FDS beriet die Gemeindefachstellen bei einzelnen Vorabkonsultationen. Weitere Themen waren Office 365 in Schulen und Verwaltung, Datenbekanntgabe ins Ausland, kantonale Einwohnerdatenplattform, Datenbekanntgabe an Contact Tracing und Zuständigkeitsfragen.

2 Personelles und Ressourcen

Die FDS verfügte im Berichtsjahr über 150 Stellenprozente. Personell ergaben sich keine Veränderungen. Die Auslastung war wie bereits in den Vorjahren gross: Einerseits war die Anzahl der Einzelanfragen höher: Die FDS bearbeitete zahlreiche Anfragen vor allem aus dem Schulbereich, die mit der Covid-19-Pandemie zusammenhingen. Gegenüber früher sind diese Anfragen häufig komplex und erfordern viel Zeit. Noch komplexer und zeitintensiver sind – wie erwartet – die Vorabkonsultationen. Die Zusammenarbeit mit verschiedenen Stellen innert den gesetzlich vorgesehenen Fristen ist sehr anspruchsvoll. Die FDS ist bestrebt, die Bearbeitungsdauer möglichst kurz zu halten. Muss allerdings ein sehr technisches und komplexes Vorhaben beurteilt werden und sind gleichzeitig etliche andere Pendenzen zu bearbeiten, ist die gesetzlich vorgesehene Frist zu knapp. Eine Besonderheit bei Vorabkonsultationen ist, dass Beratung und Beurteilung sich über einen längeren Zeitraum erstrecken können und auch deshalb erhebliche Ressourcen beanspruchen. Dank der ausgezeichneten Zusammenarbeit im Team konnte die einmal mehr steigende Arbeitslast bewältigt werden. Sollte diese weiter ansteigen, könnte deren Bewältigung mit den derzeitigen Stellenprozenten allerdings schwierig werden. Es würde sich dann auch die Frage nach einer IT-Fachperson bei der FDS stellen.⁸

⁸ Vgl. Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2019, S. 15 (32.20.03).

3 Ausblick

3.1 Personenregister

Ein grösseres Projekt im Zusammenhang mit E-Government sind das Datenmanagement Einwohnende (DME) und der Aufbau eines zentralen Personenregisters für natürliche und juristische Personen. Mit eGovernment St.Gallen digital. und der Gemeindefachstelle St.Gallen wurden die Anforderungen für die Datenaustauschvereinbarung besprochen. Eine Datenaustauschvereinbarung ist nötig, weil das Gesetz über E-Government (sGS 142.3) nur Kanton und politische Gemeinden berechtigt, ohne Vereinbarung Daten auszutauschen. In diesem Zusammenhang soll auch ein zentrales Personenregister als zentrale Datenhaltung erstellt werden. Die Ausgestaltung des Datenkatalogs ist aktuell in Arbeit.

3.2 Kantonale Einwohnerdatenplattform

Wie bereits im letzten Tätigkeitsbericht erwähnt, wird die FDS stichprobenweise die Zugriffsberechtigungen auf die Einwohnerdatenplattform prüfen. Seit der Revision der Verordnung über die kantonale Einwohnerdatenplattform (sGS 453.11) nimmt die FDS vorgängig keine Stellung mehr dazu, welche öffentlichen Organe auf welche Datenfelder zugreifen, sondern die Ermächtigung erfolgt über das jeweils oberste Leitungsorgan.

3.3 Prüfprogramm 2021

Die FDS legt für das Jahr 2021 untenstehendes Prüfprogramm fest:

1. Arbeitsbesuch bei einer Gemeindefachstelle für Datenschutz;
2. Chatbot Handelsregisteramt;
3. Lernfördersysteme;
4. Schengenkontrolle beim Migrationsamt.

4 Antrag

Wir beantragen Ihnen, Herr Präsident, sehr geehrte Damen und Herren, auf den Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2020 einzutreten.

Kantonale Fachstelle für Datenschutz

Corinne Suter Hellstern, Leiterin