# Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2019

vom 25. Februar 2020

## Inhaltsverzeichnis

## Zusammenfassung

*Am 25. Juni 2019 trat der Nachtrag zum Datenschutzgesetz in Vollzug. Damit wurde die Stellung der Datenschutzfachstellen gestärkt. Zudem wurden neue Instrumente wie die Datenschutz-Folgenabschätzung (DSFA) und die Meldepflicht bei Datenschutzverletzungen geschaffen. Erste Auswirkungen des revidierten DSG zeigten sich im vermehrten Informationsbedarf der öffentlichen Organe zur DSFA. Bei der DSFA geht es darum, das Risiko eines Projekts für die Grundrechte der betroffenen Personen abzuschätzen und darzulegen. Ergibt sich ein hohes Risiko, muss das Projekt der Fachstelle für Datenschutz (FDS) zur Vorabkonsultation vorgelegt werden. Im Berichtsjahr bearbeitete die FDS erste Vorabkonsultationen, so zur Frage der Datenbearbeitung bei der Nutzung von Mobilen Tablets.*

*Eine weitere Aufgabe der FDS ist die Bearbeitung von Einzelanfragen. Die FDS behandelte im Berichtsjahr 217 Anfragen. Themen waren einmal mehr Videoüberwachung und Cloud. Bei der Videoüberwachung besteht ein Konsens, dass eine gesetzliche Grundlage für die Videoüberwachung durch kantonale Stellen geschaffen werden soll. Beim Thema Cloud beschäftigte vor allem die Auswirkung des «Cloud Act», ein US-amerikanisches Gesetz, wonach US-Behörden ohne Einhaltung des internationalen Rechtswegs auch auf Server eines US-amerikanischen Unternehmens Zugriff nehmen können, wenn diese sich ausserhalb der USA befinden. Weitere Themen bei den Einzelanfragen waren das Krebsregister, der Zugriff auf das elektronische Personaldossier und die Archivierung von Fallakten.*

*Die kantonale Einwohnerdatenplattform (KEWR) war für die FDS immer wieder Thema: Das Verfahren für die Zugriffsberechtigungen auf KEWR wird geändert. Neu bestimmen die obersten leitenden Stellen für ihre Organisation, welche öffentlichen Organe auf KEWR zugreifen dürfen. Die leitenden Personen dieser öffentlichen Organe bezeichnen die zugriffsberechtigten Personen und den Umfang der Zugriffsberechtigung. Die FDS nimmt inskünftig nicht mehr Stellung zu den einzelnen Anträgen, sondern wird stichprobenweise kontrollieren, wie die Zugriffs-Thematik gehandhabt wird.*

*Auch im Berichtsjahr führte die FDS Prüfungen durch: Sie prüfte im Rahmen einer Schengen-Kontrolle bei der Polizei die Organisation der Zugriffsberechtigung und die Sensibilisierung. Weiter prüfte sie die Anwendung einer Fachapplikation, die den Rechtsabteilungen verschiedener Departemente als Wissensdatenbank dient.*

*Zum Aufgabenkatalog der FDS gehört die Aufsicht über die Gemeindefachstellen für Datenschutz. Im Berichtsjahr stattete die FDS der Gemeindefachstelle Flawil einen Arbeitsbesuch ab. Themen waren vor allem die Ressourcen und die Nachfolgeregelung, da der Fachstellenleiter voraussichtlich per Ende 2020 zurücktritt.*

*Im Berichtsjahr schloss die FDS eine Leistungsvereinbarung mit dem katholischen Konfessionsteil ab. Sie wird ab dem Jahr 2020 für diesen als Datenschutzfachstelle wirken.*

*Es sind nicht mehr zahlreiche Einzelanfragen, welche die Arbeit der FDS prägen. Vielmehr sind es sehr komplexe Fragen mit vielfältigen Bezügen vor allem zu technischen, aber auch gesellschaftlichen Entwicklungen. Die FDS begrüsst diese Entwicklung und es wird darauf hingewirkt, dass sich dieser Trend auch in Zukunft weiter fortsetzt.*

Herr Präsident
Sehr geehrte Damen und Herren

Die kantonale Fachstelle für Datenschutz (FDS) berichtet dem Kantonsrat jährlich über ihre Tätigkeit. Der Kantonsrat nimmt vom Bericht Kenntnis.[1] Der Bericht an den Kantonsrat hat dieselbe Stellung wie der Geschäftsbericht der Regierung nach Art. 5a des Staatsverwaltungsgesetzes (sGS 140.1).[2] Der vorliegende Bericht gibt Rechenschaft über die Tätigkeit der FDS im Jahr 2019.

# 1 Aufgaben

## 1.1 Revidiertes Datenschutzgesetz

Am 25. Juni 2019 trat der Nachtrag[3] zum Datenschutzgesetz (sGS 142.1; abgekürzt DSG) in Vollzug. Damit wurde die Stellung der Datenschutzfachstellen gestärkt. Sie erhielten zusätzliche Instrumente wie die Befugnis, Anordnungen zu erlassen; Verletzungen der Datensicherheit, sofern sie nicht leicht sind, müssen den Fachstellen gemeldet werden. Öffentliche Organe müssen bei Datenbearbeitungen, die ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen können, vorgängig eine Datenschutz-Folgenabschätzung (DSFA) machen. Zudem stehen sie stärker in der Verantwortung, indem sie die Einhaltung der Datenschutzbestimmungen beweisen müssen. Bei der Beschaffung von Personendaten muss das öffentliche Organ neu die betroffene Person informieren.

Erste Auswirkungen des revidierten DSG zeigten sich im vermehrten Informationsbedarf der öffentlichen Organe zur DSFA. Bei der DSFA geht es vereinfacht gesagt darum, das Risiko eines Projekts für die Grundrechte der betroffenen Personen abzuschätzen und darzulegen, welche Massnahmen für den Schutz getroffen wurden. Ergibt sich ein hohes Risiko, muss das Projekt der FDS zur Vorabkonsultation vorgelegt werden. Eine zentrale Frage ist, welche Datenbearbeitungen ein «hohes Risiko» für die Grundrechte der betroffenen Personen mit sich bringen können. Die FDS hat diesen Begriff in einem Merkblatt konkretisiert.[4] Der Begriff bleibt allerdings abstrakt. Zudem kann er sich mit der raschen technologischen Entwicklung schnell verändern. Praxis und Rechtsprechung werden zeigen, welche konkreten Fälle darunterfallen. Zur DSFA stellen sich auch weitere Fragen wie beispielsweise «Was sind die Konsequenzen für das öffentliche Organ, wenn es eine DSFA durchführen müsste, dies aber nicht tut? Was passiert, wenn das öffentliche Organ ein hohes Risiko feststellt, das Vorhaben aber nicht zur Vorabkonsultation vorlegt? » Auch diese Fragen werden Praxis und Rechtsprechung beantworten.

Führt ein Vorhaben eines öffentlichen Organs zu einem hohen Risiko, muss es der FDS – wie oben erwähnt – zur Vorabkonsultation vorgelegt werden. Bereits bisher mussten Vorhaben mit «besonderen Risiken» vorab durch die FDS geprüft werden. Die öffentlichen Organe befolgten dies bisher nur selten, obwohl die FDS immer wieder darauf verwies. Die im Berichtsjahr bearbeiteten drei Vorabkonsultationen lassen hoffen, dass dieser Pflicht inskünftig mehr nachgelebt wird. Die FDS wird auch beständig weiter über diese Pflicht informieren. Neu sind für die Vorabkonsultationen Fristen vorgesehen. So hat eine Vorabkonsultation in der Regel innert zwei Wochen, längstens innert sechs Wochen zu erfolgen. Die Richtlinie der Europäischen Union[5], die aufgrund

1 Art. 36 Abs. 2 des Datenschutzgesetzes (sGS 142.1; abgekürzt DSG).

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

3 nGS 2019-043.

4 https://www.sg.ch/sicherheit/datenschutz/merkblaetter-und-arbeitshilfen.html

5 Richtlinie 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhü-

des Schengen-Assoziierungsabkommens[6] umgesetzt werden musste, sieht eine Frist von sechs bis zehn Wochen vor.[7] Die bisherigen Erfahrungen haben gezeigt, dass die Einhaltung der kantonal vorgesehenen Frist sehr anspruchsvoll ist: Einerseits muss sich die FDS in die jeweilige Materie einarbeiten, um die Datenbearbeitungen nachvollziehen und beurteilen zu können. Anderseits erfordern die Vorabkonsultationen eine Beurteilung der technischen Aspekte, was den Einbezug des Informationssicherheitsbeauftragten des Dienstes für Informatikplanung (DIP) erforderlich macht. Komplexe Materie und Zusammenarbeit brauchen Zeit. Es ist sehr fordernd, ein Projekt, an welchem Fachleute längere Zeit arbeiten, in so kurzer Frist in einem sachfremden Gebiet zu beurteilen. Jedenfalls bewirken diese kurzen Fristen einen Druck auf die Ressourcen.

Eine Meldung einer Datenschutzverletzung ging im Berichtsjahr nicht ein, weshalb dazu noch keine Praxis besteht. Es stellt sich die Frage, was die Folgen einer Meldung sind. Dies dürfte unter anderem von der Schwere der Verletzung abhängen. Auch die Anordnung kam noch nicht zur Anwendung.

## 1.2 Einzelanfragen

### 1.2.1 Themen

Wie bereits in den vergangenen Jahren interessierten die Themen Videoüberwachung und Cloud. Die Videoüberwachung wurde unter anderem von der Delegation Aufsicht Datenschutz der Staatswirtschaftlichen Kommission des Kantonsrates thematisiert. Derzeit gibt es keine gesetzliche Grundlage, die es kantonalen Stellen erlauben würde, Videoüberwachung einzusetzen. Aktuell besteht ein Konsens unter den Beteiligten, dass eine solche Grundlage geschaffen werden soll, entweder im Rahmen eines zukünftigen Nachtrags zum Polizeigesetz (sGS 451.1) oder zum Datenschutzgesetz, was die FDS begrüsst. Mehrere Anfragen betrafen das Krebsregister und den Zugriff auf das E-Dossier, das elektronische Personaldossier. Nachfolgend eine Darstellung dieser Fälle und weiterer allgemein interessierender Anfragen.

*Cloud*

Beim Thema Cloud waren vor allem die Konsequenzen des «Cloud Act»[8] für eine Auslagerung einer Datenbearbeitung Thema: Beim «Cloud Act» handelt es sich um ein US-Gesetz, das US-Behörden erlaubt, auf Server im Ausland zuzugreifen, falls es sich um einen Anbieter handelt, der dem «Cloud Act» untersteht (im Wesentlichen US-Unternehmen). US-Behörden können also ohne den Weg über die internationale Rechtshilfe auf Server in Europa – beispielsweise in Irland oder den Niederlanden, aber auch in der Schweiz – zugreifen. Derzeit fehlt es an Rechtsprechung und Praxis, um abschätzen zu können, wie der «Cloud Act» angewendet wird. Deshalb vertritt die FDS die Ansicht, dass besonders schützenswerte Personendaten und solche, die dem Berufsgeheimnis unterstehen, nicht an ein dem «Cloud Act» unterstehendes Unternehmen ausgelagert werden dürfen, auch wenn der Server in Europa bzw. in der Schweiz steht. Die Auslagerung von Personendaten in eine Cloud ist eine Bearbeitung durch Dritte[9] mit besonderen Risiken. Es müssen die im DSG genannten Voraussetzungen erfüllt sein. Zusätzlich stellen sich insbesondere drei weitere Fragen: Welches Recht wird angewendet und welcher Gerichtsstand gilt? Wo wird die Cloud-Infrastruktur betrieben? Wie wird verschlüsselt und das Schlüsselmanagement gehandhabt? Bei einer beabsichtigten Auslagerung in die Cloud muss für jeden einzelnen Fall eine Risikobeurteilung gemacht werden. Wichtig ist, dass das öffentliche Organ dem Geschäftspartner

tung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Amtsblatt der EU Nr. L 119/89 vom 4. Mai 2016), nachfolgend Richtlinie 2016/680.

6 SR 0.362.31.

7 Art. 28 Abs. 5 Richtlinie 2016/680.

8 https://www.congress.gov/bill/115th-congress/house-bill/4943.

9 Art. 9 DSG. Siehe dazu auch Merkblatt Outsourcing, abrufbar unter https://www.sg.ch/sicherheit/datenschutz/merkblaetter-und-arbeitshilfen.html

vertraut. Im Fall der Auslagerung muss die Leitung des öffentlichen Organs schriftlich bestätigen, dass sie die Risiken verstanden hat und das Restrisiko übernimmt. Aufgrund des «Cloud Act» hat auch Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, ihr Positionspapier zu Cloud aktualisiert.[10] Die Position von Privatim deckt sich weitgehend mit der Praxis der FDS.

Ob die Auslagerung von besonders schützenswerten Personendaten und Personendaten, die dem Berufsgeheimnis unterstehen, in einen Cloudservice in der *Europäischen Union* – deren Länder gemäss Staatenliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)[11] über ein der Schweiz gleichwertiges Datenschutzniveau verfügen – zulässig ist, hängt von der konkreten Risikobeurteilung im Einzelfall ab.

*Krebsregister*
Auf 1. Januar 2020 trat das neue Krebsregistrierungsgesetz des Bundes mit der dazu gehörenden Verordnung in Kraft[12]. Daher musste das Krebsregister sein Datenschutzkonzept anpassen. Die FDS unterstützte die Stelle dabei. Die Anpassung betraf unter anderem das Widerspruchsrecht von Patientinnen und Patienten gegen eine Registrierung im Krebsregister. Zudem war fraglich, ob eine Abspeicherung des Krebsregisters beim Bundesamt für Informatik rechtmässig sei, was die FDS bejahte. Eine weitere Frage betraf die Registrierung der Patientinnen und Patienten bereits vor Inkrafttreten bzw. Berücksichtigung des Widerspruchsrecht. Dies ist nicht zulässig, die Frist für das Widerspruchsrecht der Patientinnen und Patienten von drei Monaten muss gewahrt werden. Ein weiteres Thema war die Zugriffsregelung auf die kantonale Einwohnerdatenplattform (KEWR). Bis anhin hatte das Krebsregister keinen direkten Zugriff, was geändert werden soll.

*Zugriff E-Dossier*
Mehrere Anfragen betrafen den Zugriff auf E-Dossier, das elektronische Personaldossier. Die Finanzkontrolle fragte an, ob es zulässig sei, dass sie Zugriff auf die E-Dossiers der Angestellten im Kanton erhalten dürfe. Im Zentrum dieser Anfrage stand die Thematik des Abrufverfahrens. Nach verschiedenen Abklärungen und Gesprächen mit den Verantwortlichen kam die FDS zum Schluss, dass das Vorhaben kein Abrufverfahren darstellt, da nicht auf alle E-Dossiers systematisch in Selbstbedienung zugegriffen würde. Die Finanzkontrolle konnte bisher die Personaldossiers vor Ort einsehen. Das Einsehen elektronischer Dossiers entspricht dem heutigen Stand der Technik. Nach Auffassung der FDS verfügt die Finanzkontrolle über eine hinreichende formellgesetzliche Grundlage, um punktuell und für eine beschränkte Zeit besonders schützenswerte Personendaten auf elektronischem Weg einzusehen. Aus datenschutzrechtlicher Sicht können die Zugriffe demnach in engen Grenzen erfolgen (u.a. dürfen nur die für die gesetzliche Aufgabenerfüllung unentbehrlichen Daten eingesehen werden, das Personalamt gewährt die Zugriffe und entzieht sie nach einer Dauer von vier Wochen, die Zugriffe müssen protokolliert werden).

Weiter stellte sich bei E-Dossier die Frage, ob es in gewissen Fällen zulässig sei, dass die stellvertretende Person auf das Dossier der ihr vorgesetzten Person Zugriff erhalte. Nach Ansicht der FDS ist dies nicht der Fall: Es ist keine Konstellation denkbar, in der dieser Zugriff gerechtfertigt erscheint bzw. die stellvertretende Person die Daten der vorgesetzten Person benötigt.

*Archivierung Fallakten*
Eine Beratungsstelle wandte sich an die FDS und wollte wissen, ob sie trotz gesetzlicher Schweigepflicht verpflichtet sei, ihre Akten dem Staatsarchiv anzubieten. Die FDS prüfte diese Anfrage einerseits vor dem Hintergrund der Derogation (Normenkollision) beider Bestimmungen und an-

10 Vgl. https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf
11 Vgl. https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html
12 SR 818.33 und SR 818.331.

derseits vor dem Hintergrund der Verhältnismässigkeit. Die beiden Bestimmungen regeln unterschiedliche Sachverhalte, womit keine Normenkollision besteht. Die Verhältnismässigkeitsprüfung hat gezeigt, dass sowohl die Interessen des Staatsarchivs als auch jene der Beratungsstelle zu berücksichtigen sind, ohne dass das eine Interesse einseitig zulasten des anderen durchgesetzt werden darf. Unter Einhaltung gewisser Bedingungen erachtete die FDS das Anbieten als zulässig: Der Zugang zum Archivgut darf konsequent erst nach Ablauf der Schutzfrist erfolgen und im Fall von besonders schützenswerten Personendaten soll sie verlängert werden. Zudem müssen der betroffenen Person nach Ablauf der Aufbewahrungsfrist die Akten herausgegeben werden, falls diese dies beantragt.

*Informationsfilter*
Die FDS befasste sich im Zusammenhang mit dem Projekt «Schulen ans Internet» mit der Informationsfilterung. Die meisten Schulen stellten die Verschlüsselung ihrer Webseiten von «http» auf «https» um. Damit der Fernmeldedienstanbieter die Inhalte der aufgerufenen Webseiten zum Schutz der Schülerinnen und Schüler wieder filtern kann, muss er die https-Verschlüsselung aufbrechen können. Er verlangte dabei die Einwilligung der kantonalen Datenschutzbeauftragten. Ein wichtiger Diskussionspunkt in diesem Zusammenhang war, welche Webseitenkategorien (thematisch) nicht gefiltert werden sollten. Die FDS vertritt die Ansicht, dass besonders schützenswerte Personendaten von der Filterung ausgenommen werden sollten.

Bei den Medienanfragen war mehrmals die Videoüberwachung Thema, wobei es entweder um Private ging oder um Videoüberwachung durch eine Gemeinde. In diesen Fällen sind der EDÖB) und die regionalen Datenschutzfachstellen zuständig. Mehrmals Thema war auch WhatsApp an Schulen.

### 1.2.2 Zahlen
Die FDS behandelte im Jahr 2019 217 Einzelanfragen, im Vorjahr waren es 248. Damals war der Vollzug der Datenschutz-Grundverordnung Thema. Dies wurde in den Medien stark thematisiert, was zu einigen Anfragen an die FDS führte. Im Berichtsjahr gab es nichts Vergleichbares, das zu zahlreichen zusätzlichen Anfragen führte. Die FDS war in gut 70 Prozent der Fälle für die Bearbeitung zuständig.

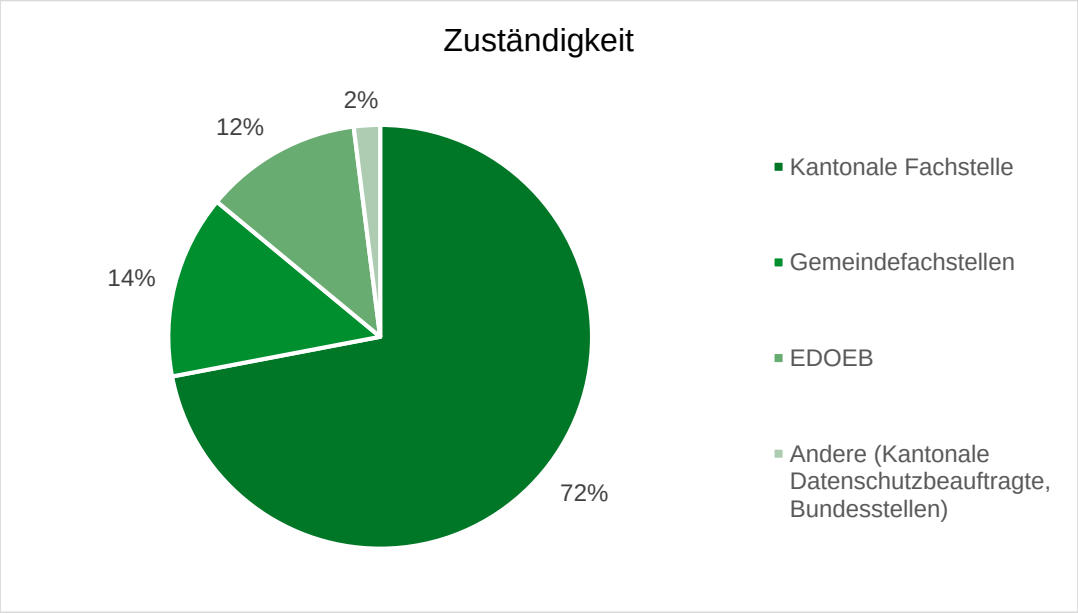

Abb. 1: Zuständigkeit für Einzelanfragen in Prozent, 2019

Bei der Herkunft der Einzelanfragen fällt auf, dass sich mehr Private (private Personen und private Unternehmen) an die FDS wandten, währenddem die Anfragen der Gemeindefachstellen um sieben Prozent abnahmen. Letzteres könnte darauf zurückzuführen sein, dass die Leiterinnen und Leiter der Gemeindefachstellen erfahrene Personen sind, welche die Gemeindefachstellen seit mehreren Jahren leiten. Sie verstehen deshalb auch mit komplexeren Anfragen umzugehen. Die Zunahme bei den Privaten könnte sich damit erklären, dass einerseits die Sensibilität bei betroffenen Personen einmal mehr zugenommen hat. Zudem ist es heute viel selbstverständlicher, beim Datenschutz die eigenen Rechte wahrzunehmen.

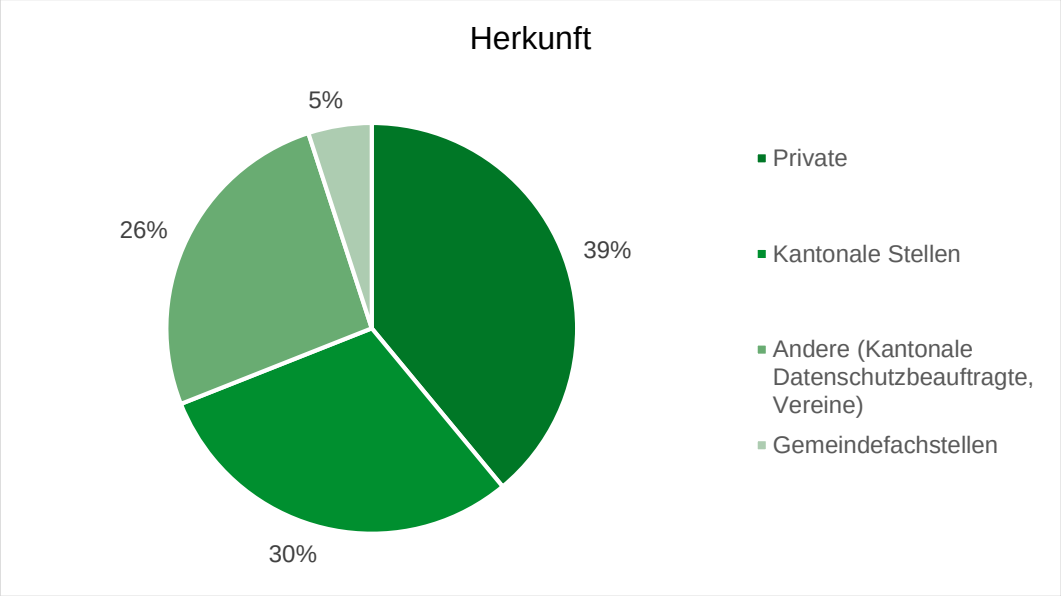


Abb. 2: Herkunft der Einzelanfragen in Prozent, 2019

Wie bereits im Vorjahr beanspruchten die meisten Einzelanfragen zwischen einer halben und fünf Stunden Arbeit. Innerhalb dieses Segments gab es gegenüber dem Vorjahr eine Verschiebung zu Gunsten derjenigen Anfragen, die mehr als eine Stunde beanspruchten.

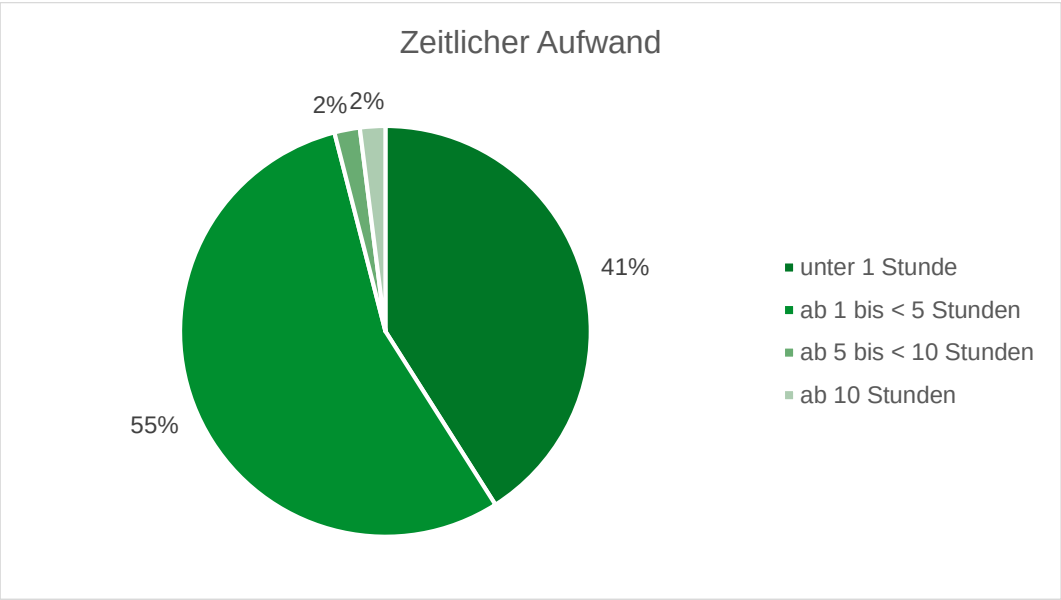


Abb. 3: Bearbeitungsaufwand von Einzelanfragen in Prozent, 2019

## 1.3 Rechtsetzung

*Verordnung über die kantonale Einwohnerdatenplattform*

Das Verfahren für die Zugriffsberechtigung auf die kantonale Einwohnerdatenplattform (KEWR) sollte geändert werden: Neu bestimmen die obersten leitenden Stellen für ihre Organisation, welche öffentlichen Organe auf KEWR zugreifen dürfen. Die leitenden Personen dieser öffentlichen Organe bezeichnen wiederum die zugriffsberechtigten Personen und den Umfang der Zugriffsberechtigung. Die FDS nimmt nicht mehr wie bisher Stellung zu den Anträgen der einzelnen Stellen. Sie sprach sich dennoch nicht gegen diese Änderung aus: Mit dem neuen System wird die Verantwortung der leitenden Personen gestärkt, dies ist im Sinn des revidierten DSG. Die Zugriffsberechtigungen werden veröffentlicht. Die FDS wird inskünftig stichprobenweise kontrollieren, ob die Stellen das Zugriffskonzept einhalten. Aufgrund der hohen Missbrauchsgefahr, die ein solches Abrufverfahren mit sich bringt, hat die FDS in ihrer Stellungnahme darauf hingewiesen, die Anzahl der in KEWR bearbeiteten Personendaten klein zu halten. Der Zweck der Einwohnerdatenplattform soll restriktiv definiert werden. Grosse Datenplattformen mit umfangreichen Datensätzen, die für sehr viele Zwecke genutzt werden, bieten eine potenziell grössere Angriffsfläche. Zudem stellte sich die Frage nach dem Zusammenhang zum Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen, das der Bund plant. Die revidierte Verordnung über die kantonale Einwohnerdatenplattform (sGS 453.11) ist in Vollzug und wird seit dem 1. Januar 2020 angewendet.

*Adressdienstgesetz*

Die FDS nahm zum Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen Stellung. Damit sollen öffentliche Verwaltungen von Bund, Kantonen und Gemeinden entlastet und administrative Prozesse vereinfacht werden. Kritikpunkte waren dabei einerseits die Notwendigkeit bzw. der Bezug zur gesetzlichen Aufgabenerfüllung und anderseits die systematische Verwendung der AHV-Nummer, anhand derer die Verknüpfung erfolgen soll.

*Asylverordnung*

Eine Revision der kantonalen Asylverordnung (sGS 381.12) sollte den Einsatz einer Videoüberwachung in einem Ausreise- und Notfallzentrum ermöglichen. Die explizite Rechtsgrundlage war notwendig, da die Norm im eidgenössischen Asylgesetz (SR 142.31) nicht konkret genug ausformuliert war. Grundsätzlich wäre für den Einsatz von Videoüberwachung eine Rechtsgrundlage auf Gesetzesstufe notwendig. Da sich die Bewohnerinnen und Bewohner eines Ausreise- und Notfallzentrum in einem Sonderstatusverhältnis zum Staat befinden, genügt eine Rechtsgrundlage auf Stufe Verordnung.[13] Hingegen erachtete die FDS die Aufbewahrungsfrist von 100 Tagen als zu lang. Zudem muss ein Reglement erlassen werden. Darin muss unter anderem geregelt werden, welche Bereiche überwacht werden und wer Zugriff auf die Aufnahmen hat. Diese Zugriffsberechtigungen müssen restriktiv gehandhabt werden. Das Reglement sollte zudem – ähnlich wie die Hausordnung – veröffentlicht werden.

Im Weiteren hat die FDS zu folgenden Erlassentwürfen und Vorhaben Stellung genommen:
– Schengen-Evaluierung;
– Berufsbildungsverordnung;
– DNA-Profil-Gesetz.

13 BGE 139 I 280.

## 1.4 Vorabkonsultationen

*Cloud Universität St.Gallen*

Die Universität St.Gallen beabsichtigte, vermehrt Anwendungen in der Cloud zu halten und nicht mehr vor Ort (on premise). Dieses Vorhaben legte die Universität der FDS zur Vorabkonsultation vor. Anwendungen mit besonders schützenswerten Personendaten oder Daten, die dem Berufsgeheimnis unterstehen, sollten nicht ausgelagert werden. So sollten die Personaldossiers nicht in der Cloud im Ausland gespeichert werden. Die FDS hielt fest, dass das Vorhaben zulässig sei, wenn im Wesentlichen folgende Bedingungen eingehalten werden: Besonders schützenswerte Personendaten und Persönlichkeitsprofile dürfen – wie vorgesehen – nicht in der fraglichen Cloud bearbeitet werden. Es soll mit dem Anbieter (ein US-Unternehmen) vereinbart werden, wie im Fall eines Herausgabegesuchs an eine US-Behörde vorzugehen ist und die Universitätsleitung muss schriftlich bestätigen, dass sie die Risiken verstanden hat und das Restrisiko übernimmt.

*Cloud-Lösung für Schutzplatzangebot Amt für Militär und Zivilschutz*

Die Kantone haben die Aufgabe, ein ausgewogenes Schutzplatzangebot zu gewährleisten. Ohne eine Informatik-Lösung kann die zuständige Amtsstelle diese Aufgabe nicht erfüllen. Die bis anhin verwendete Software eines Schweizer Unternehmens wurde bei der Abraxas gehostet. Neu bot der Softwareanbieter eine eigene Cloud-Lösung mit Serverstandort in der Schweiz an. Die Cloud ist gemäss ISO 27001 und ISO 9001 zertifiziert. Die FDS prüfte die Risikobeurteilung des Amtes für Militär und Zivilschutz. Aufgrund der Risikobeurteilung und der vorgelegten Unterlagen sprach nichts gegen eine Durchführung des Projekts.

*Mobile Tablets Kantonsforstamt*

Ziel des Projekts beim Kantonsforstamt war, die Applikation, mit der Försterinnen und Förster georeferenzierte Massnahmen im Wald ergreifen, offline verwenden zu können, weil der Handyempfang an manchen Orten nicht vorhanden ist. Datenschutzrechtliche Risiken für die betroffene Person bestanden einerseits darin, dass Personendaten auf dem Tablet offline zur Verfügung stehen und (von unberechtigten Dritten) eingesehen werden können und anderseits der Gefahr der Installation von Malware bei der automatischen Datenverbindung. Die FDS stellte fest, dass die Datenbearbeitung an Orten ohne Handy-Empfang für die gesetzliche Aufgabenerfüllung erforderlich ist. Den mit diesem Projekt einhergehenden Restrisiken wurden mit geeigneten Massnahmen (Durchführung von Sicherheitsmassnahmen oder der Abschluss eines Hosting- und Operations-Vertrags einschliesslich Geheimhaltungsvereinbarung) entgegengewirkt. Management und Hosting wird von Dritten wahrgenommen. Dabei handelt es sich bei beiden um Schweizer Unternehmen. Den eingereichten Unterlagen konnte nichts entnommen werden, was die geplante Umsetzung des Projekts aus datenschutzrechtlicher Sicht hätte ausschliessen können.

## 1.5 Prüftätigkeit

*Schengen-Kontrolle*

Die FDS führte im Berichtsjahr zusammen mit dem DIP eine Schengen-Kontrolle bei der Kantonspolizei durch. Nach dem Übereinkommen zur Durchführung des Übereinkommens von Schengen[14] bezeichnet jede Vertragspartei eine Kontrollinstanz, deren Aufgabe darin besteht, nach Massgabe des jeweiligen nationalen Rechts den Bestand des nationalen Teils des Schengener Informationssystems unabhängig zu überwachen und zu prüfen, ob durch Verarbeitung und Nutzung der im Schengener Informationssystem (SIS) gespeicherten Daten die Rechte des Betroffenen nicht verletzt werden (Art. 114 Abs. 1 des Übereinkommens). Die FDS ist für die Prüfung bei kantonalen Stellen zuständig.[15]

14 Schengener Durchführungsübereinkommen, Amtsblatt der EU Nr. L 239/19 vom 22. September 2000.

15 Art. 30 Abs. 1 Bst. a i.V.m. Art. 24 Abs. 1 DSG.

FDS und DIP führten Querschnittsprüfungen zur Organisation der Zugriffsberechtigung und zur Sensibilisierung durch. Der Umgang der Kantonspolizei mit dem SIS machte diesbezüglich einen guten Eindruck: Die Abläufe sind definiert, die Rechtmässigkeit ist gegeben. Auch die Verhältnismässigkeit scheint gewahrt. Der Zugriff auf das Fahndungssystem RIPOL bedeutet automatisch auch Zugriff auf das SIS. Diese Zugriffsberechtigung erscheint etwas weit. Es handelt sich allerdings um eine gesamtschweizerische Regelung in einem Bundeserlass (Art. 4 Abs. 5 Bst. a der eidgenössischen N-SIS-Verordnung [SR 362.0]). Aus Praktikabilitätsgründen ist die Lösung nachvollziehbar. In gewissen Fällen können stellvertretende Abfragen für Arbeitskolleginnen und -kollegen gemacht werden; zum Beispiel durch die Kantonale Notrufzentrale für Kolleginnen und Kollegen im Einsatz. Diese Abfragen konnte die Kantonspolizei begründen und erschienen dem Prüfteam nachvollziehbar. Dank dem jährlichen E-Learning des Kantons zur Informationssicherheit und zum Datenschutz werden die Mitarbeitenden in diesen beiden Themen regelmässig geschult. Insgesamt wurden keine Abweichungen festgestellt und es waren keine Empfehlungen erforderlich.

*Applikation Dorian beim Baudepartement*
Im Berichtsjahr prüfte die FDS zusammen mit dem DIP die Fachapplikation Dorian. Dorian ist eine Wissensdatenbank, in der unter anderem nicht anonymisierte Entscheide, Rechtsauskünfte, Urteile und Verfügungen gesammelt werden. Dorian dient den Rechtsabteilungen verschiedener Departemente zur Bearbeitung von Entscheiden. Zweck ist, ein effizientes Wissensmanagement und eine einheitliche Rechtsprechung zu gewährleisten. Verantwortlich für die Fachanwendung ist die Rechtsabteilung des Baudepartementes. Dorian ist kein eigenständiges System, sondern in der bestehenden Microsoft-Sharepoint-Umgebung integriert und nutzt diese Infrastruktur. Zugriffe gibt es sowohl innerhalb des Departementes als auch departementsübergreifend.

Die Bearbeitung der Prüfung ist noch nicht abgeschlossen, Baudepartement und FDS diskutieren noch verschiedene Fragen. Festgehalten werden kann indes, dass es sich bei Dorian um ein Abrufverfahren handelt, das einer Rechtsgrundlage für den Abruf bedarf.[16] Diese Anforderung besteht deshalb, weil Empfängerinnen und Empfänger der Daten diese in «Selbstbedienung» beschaffen können.[17] Damit besteht eine erhöhte Gefahr einer Verletzung der Persönlichkeitsrechte. Wie hoch diese Gefahr ist, hängt allerdings wesentlich von der Ausgestaltung des Abrufverfahrens ab. Seit Erlass dieser Bestimmung im Jahr 2008 ist das Abrufverfahren beinahe alltäglich geworden. Es fehlt denn auch häufig die explizite Regelung für das Abrufverfahren, so auch bei Dorian. Da allerdings für eine Datenbekanntgabe ohnehin eine Rechtsgrundlage erforderlich ist, erachtet es die FDS wenigstens bei weniger schwerwiegenden Eingriffen in die Grundrechte als entbehrlich, zusätzlich eine solche für das Abrufverfahren zu schaffen. Eine stichprobenweise Prüfung bei verschiedenen Kantonen hat ergeben, dass diese über keine vergleichbare Bestimmung verfügen. Der Bund hat zwar eine solche, sie soll aber mit der Revision des eidgenössischen Datenschutzgesetzes (SR 235.1) gestrichen werden, «weil sie im digitalen Zeitalter überholt erscheint»[18].

*Zutrittsmanagement Spital*
Ein Spital führt auf das Jahr 2020 ein neues Schliesssystem ein. Dabei stellen sich auch Fragen des Datenschutzes. Die Prüfung soll einerseits zeigen, wie das Zutrittsmanagement funktioniert. Anderseits soll geprüft werden, ob die geltenden datenschutzrechtlichen Bestimmungen eingehalten werden. Derzeit wertet die FDS den im Dezember retournierten Fragebogen aus.

16 Art. 15 DSG.

17 ABl 2008, 2299 ff., 2318.

18 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017, 7083).

## 1.6 Anzeigen

Im Jahr 2019 ging bei der FDS eine Anzeige ein. Eine private Person meldete, dass eine Liste von Personendaten einschliesslich besonders schützenswerter Personendaten im Internet ersichtlich war. Diese Liste konnte ohne Eingabe eines Passworts eingesehen werden. Der Vorfall datierte aus dem Jahr 2018. Die FDS wandte sich an die zuständige Stelle, worauf diese darlegte, welche Massnahmen ergriffen wurden, um einen weiteren solchen Vorfall zu verhindern. In Absprache mit dem DIP erachtete die FDS die getroffenen Massnahmen als genügend. In solchen Fällen behält sich die FDS künftige Kontrollen vor.

## 1.7 Empfehlungen und Massnahmen

Die FDS machte im Jahr 2019 keine Empfehlung gemäss Art. 33 DSG.

## 1.8 Gemeindefachstellen für Datenschutz

### 1.8.1 Arbeitsbesuch

Die FDS machte zusammen mit dem DIP einen Arbeitsbesuch bei der Gemeindefachstelle Flawil. FDS und DIP erörterten mit dem Fachstellenleiter folgende Themen: Ausgestaltung der Stelle, Infrastruktur inklusive Informatik, Unabhängigkeit, Aufgabenerfüllung, Zusammenarbeit und Nachfolgeregelung.

Der Fachstellenleiter leistet im Rahmen seiner zeitlichen und finanziellen Möglichkeiten gute Arbeit. Besonders zu würdigen ist seine stete Sensibilisierungsarbeit einerseits im direkten Gespräch mit den datenbearbeitenden Stellen, anderseits mit den Hinweisen auf aktuelle Abhandlungen zum Thema. Sein persönliches Interesse und Engagement für das Thema führen zu einer grossen Glaubwürdigkeit, was dem Datenschutz sehr dient. Zeitlich steht dem Fachstellenleiter etwa eine Stunde je Woche zur Verfügung. Das ist zu wenig. Dies vor allem auch mit Blick auf die neu eingeführten Instrumente wie die DSFA und die Meldung von Verletzungen der Datensicherheit. Die Berichterstattung ist institutionalisiert und auch die zeitliche Frist angemessen. Die FDS würde begrüssen, wenn der Bericht im Internet veröffentlicht würde. Der jetzige Stelleninhaber tritt voraussichtlich Ende 2020 als Datenschutzbeauftragter der Gemeinde Flawil zurück. Die Nachfolgeregelung sollte zeitig angegangen werden. Die Gemeinde ist frei in der Organisation, einzig dass eine Datenschutzfachstelle eingesetzt werden muss, ist Pflicht. Die FDS empfiehlt allerdings aufgrund der bereits gesammelten Erfahrungen eine Vereinbarung mit einer regionalen Datenschutzfachstelle abzuschliessen.

### 1.8.2 Erfahrungsaustausch

Im Berichtsjahr fanden zwei Erfahrungsaustausche mit den Gemeindefachstellen statt.

Ein Thema war Office 365: Eine Fachperson der Stadt St.Gallen präsentierte, wie Office 365 bei den städtischen Schulen verwendet wird. Ziel ist der Austausch von Informationen an einem zentralen Ort. Es soll nicht für den Austausch von sensitiven Personendaten verwendet werden. Zweites schwergewichtiges Thema war das revidierte DSG. Diesbezüglich stellten die Gemeindefachstellen noch keine Besonderheiten fest (vermehrte Anfragen, andere Themen, Komplexität). Allerdings war der Beurteilungszeitraum auch sehr kurz. Ein weiteres Thema war die Archivierung bei Gemeinden; die Zutrittsberechtigungen zu den Archiven sind teilweise sehr weit gefasst. Ausserdem gilt es sicherzustellen, dass bei Übergabe der physischen Akten an das Archiv auch die elektronische Version für die bisher datenbearbeitende Stelle nicht mehr zugänglich ist.

### 1.8.3 Übriges

Die Anfragen der Gemeindefachstellen an die FDS betrafen überwiegend Fragen zum revidierten Datenschutzgesetz. Daneben waren der Umgang mit Fotos in Kindergärten, eine Datenschutzerklärung betreffend Soziale Medien und Cloud Thema. Zudem ging eine Anfrage zur Erstellung eines Merkblatts zu Office 365 ein. Diese Anfrage wird die FDS koordinieren. Ausserdem kontrolliert die FDS, ob alle politischen, Schul- und Ortsgemeinden eine Datenschutzfachstelle eingesetzt haben.

## 1.9 Öffentlichkeitsarbeit

Im 2019 erneuerte der Kanton St.Gallen – und damit auch die FDS – seinen Internetauftritt. Die FDS erstellte zudem nach Rücksprache mit der Stelle für Lehrlingskoordination einen Clip für Lernende.[19] Der Clip stiess bei den Berufsbildungsverantwortlichen auf sehr positives Echo. Die Sensibilisierung ist im revidierten DSG explizit als Aufgabe der Fachstelle aufgeführt. Zudem erstellte die FDS eine Sequenz für das E-Learning, das alle Mitarbeitenden des Kantons absolvieren müssen. Thema waren die Neuerungen des revidierten DSG.

## 1.10 Zusammenarbeit

Das revidierte DSG sieht die Zusammenarbeit mit Organen der anderen Kantone, des Bundes und des Auslands, welche die gleichen Aufgaben erfüllen, explizit vor. Diese Zusammenarbeit findet unter anderem im Rahmen der Versammlungen von Privatim statt. Themen im Berichtsjahr waren die Aktualisierung des Positionspapiers zu Cloud, die Ressourcen der kantonalen Datenschutzbeauftragten und die neuen Instrumente DSFA und Meldepflicht bei Datenschutzverletzungen sowie die Vorabkonsultation. Daneben arbeitete die FDS auch bei konkreten Einzelanfragen oder Projekten mit anderen Datenschutzbeauftragten zusammen, beispielsweise beim Projekt «Digitaler Lesesaal» des Staatsarchivs oder bei Fragen zu den neuen Instrumenten des DSG. Regelmässig findet auch ein Austausch mit den anderen Ostschweizer Datenschutzbeauftragten statt. Die Leiterin der FDS wurde zudem auf Anfang 2020 in den Vorstand von Privatim gewählt. Daneben pflegt die FDS wie bisher den regelmässigen Austausch mit zahlreichen Stellen des Kantons und mit den Gemeindefachstellen für Datenschutz.

## 1.11 Register der Datensammlungen

Im Berichtsjahr stellten einige wenige Personen ein Einsichtsgesuch in ihre allfälligen bei der FDS vorhandenen Daten.

## 1.12 Geschäftseingänge in Zahlen

Im Berichtsjahr gingen bei der FDS 251 Geschäfte ein (Vorjahr 286). Diese Abnahme ist ziemlich deckungsgleich mit der Abnahme bei den Einzelanfragen. Die Anzahl der Eingänge bei den Projekten, den Vernehmlassungen und bei den Medienanfragen bewegen sich im Rahmen des Vorjahrs.

[19] https://youtu.be/gtQxSM7TxOM.

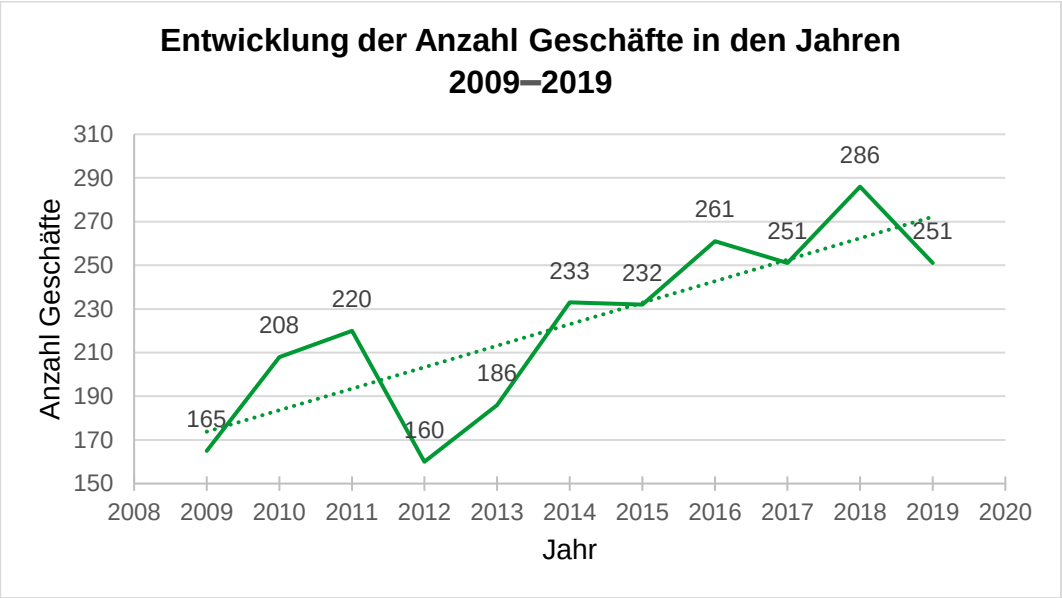


Abb. 4: Entwicklung der Geschäftszahlen der Fachstelle in den Jahren 2009 bis 2019

**Aufgabenverteilung nach Art**

Entsprechend der geringeren Anzahl eingegangener Einzelanfragen verwendete die FDS auch weniger Zeit dafür: 24 Prozent gegenüber 40 Prozent im Vorjahr. Dafür verdoppelte sich der Aufwand für die Bearbeitung von Projekten bzw. Vorabkonsultationen. Dies hängt damit zusammen, dass die eingegangenen Vorabkonsultationen die FDS aufgrund ihrer Komplexität stark beanspruchten und auch grundsätzliche Fragen diskutiert werden mussten. Zudem erforderten sie vermehrt auch die Zusammenarbeit mit anderen Stellen, insbesondere dem DIP. Auch die Öffentlichkeitsarbeit beanspruchte mehr Zeit: einerseits durch das Überarbeiten des Internet-Auftritts, anderseits durch die Erstellung des Clips für Lernende. Die übrigen Zahlen bewegen sich im Rahmen des Vorjahrs.

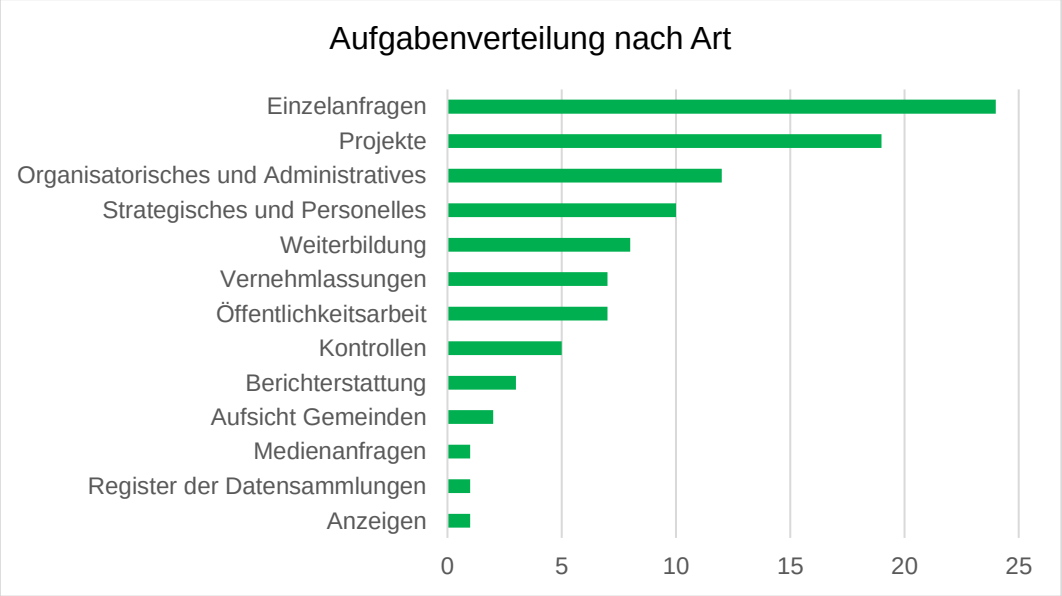


Abb. 5: Aufgabenverteilung gemäss interner Arbeitszeiterfassung in Prozent (gerundet), 2019

## 2 Personelles und Ressourcen

Die FDS verfügte im Berichtsjahr über 150 Stellenprozente. Diese teilten sich auf in ein 70-Prozent-Pensum (Leitung) und je zwei 40-Prozent-Pensen (juristische Sachbearbeitung). Dies änderte sich auch nach dem personellen Wechsel bei einer Sachbearbeiter-Stelle im Frühling nicht. Die Auslastung war wie bereits in den Vorjahren gross: Einerseits war (und ist) die Revision des DSG zu bewältigen. Dazu gehört nicht nur, dass Merkblätter erstellt und Fragen beantwortet werden mussten, sondern vor allem auch die Auseinandersetzung mit den neuen Instrumenten, die der FDS zur Verfügung stehen. Anderseits ist einmal mehr auf die weiter zunehmende Komplexität der Materie – auch im Zuge der Digitalisierung – zu verweisen. Zunehmend ist weniger die Anzahl, sondern die Art der eingehenden Geschäfte massgebend für die Beanspruchung der FDS. Die Ressourcenfrage hängt – nebst der allgemeinen Digitalisierung – unter anderem mit der Entwicklung bei den Vorabkonsultationen und der Meldung von Datenschutzverletzungen zusammen. Auch sich stellende Fragen zur DSFA und der Aufwand für allfällige Anordnungen sind nicht kalkulierbar. Erschwerend kommen die knappen Fristen bei der Vorabkonsultation hinzu, die zu einem Druck auf die Ressourcen führen und Engpässe bewirken können.

## 3 Würdigung

Revidiertes DSG, «Cloud Act», Dorian – es sind nicht mehr zahlreiche Einzelanfragen, welche die Arbeit der FDS prägen. Vielmehr sind es sehr komplexe Fragen mit vielfältigen Bezügen vor allem zu technischen, aber auch gesellschaftlichen Entwicklungen. Auch internationale Erlasse, wie erwähnt der «Cloud Act», haben in der globalisierten Welt einen Einfluss auf Datenbearbeitungen der öffentlichen Organe. Die Bearbeitung solcher Fragen erfordert sehr viel Zeit. Dies ist auch an der stark gestiegenen Beanspruchung für Projekte bzw. Vorhaben mit hohen Risiken ersichtlich. Das revidierte DSG akzentuiert diese Entwicklung mit seinen neuen Instrumenten, mit denen es bisher nur wenig Erfahrungen gibt. Immer wichtiger wird deshalb die Zusammenarbeit, welche die FDS schon seit Jahren mit verschiedenen Stellen pflegt: Häufig stellen sich bei den Datenschutzstellen dieselben Probleme, ein Austausch ist deshalb sehr wichtig. Die Mitarbeit im Vorstand von Privatim bietet eine gute Voraussetzung, diese Zusammenarbeit zu vertiefen. Die Zusammenarbeit mit IT-Fachleuten ist ebenso unerlässlich. Auch wenn Juristinnen und Juristen sowie IT-Fachleute nicht immer dieselbe Sprache sprechen, ist es umso wichtiger, am Ball zu bleiben und gemeinsame Lösungen zu suchen.

Datenschutz ist in der Mitte der Gesellschaft angekommen: Themen wie das Krebsregister oder die Videoüberwachung betreffen die ganze Gesellschaft. Ein Ziel der FDS muss sein, die öffentlichen Organe bei der Einhaltung des Datenschutzes und dem Schutz der Privatsphäre zu unterstützen. Ein wichtiges Instrument dazu ist die Sensibilisierung, die neu ausdrücklich im DSG geregelt ist. Sensibilisierung dient einerseits den öffentlichen Organen bei der Wahrnehmung ihrer Pflichten, anderseits befähigt sie die Menschen, ihr Grundrecht auf Datenschutz wahrzunehmen und dafür einzustehen.

Am Beispiel von Dorian zeigt sich, wie sich die Bewertung einer Technologie mit der Zeit ändern kann: Das Abrufverfahren gehörte vor zehn Jahren zu den Technologien, die nur wenig verbreitet waren – mit erheblichem Risikopotenzial für den Datenschutz. Heute ist die Technologie allgegenwärtig, wenn auch nach wie vor in vielen Fällen mit einem erhöhten Risiko für den Datenschutz. Eine explizite Regelung für das Abrufverfahren war damals sinn-, heute aber nicht mehr gleich wirkungsvoll. Da für eine Datenbekanntgabe ohnehin eine Rechtsgrundlage erforderlich ist, erachtet es die FDS wenigstens bei weniger schwerwiegenden Eingriffen in die Grundrechte als entbehrlich, zusätzlich eine solche für das Abrufverfahren zu schaffen.

Das revidierte DSG führte für den Datenschutz wichtige Instrumente ein wie die DSFA und die Meldepflicht bei Datenschutzverletzungen. Bei der Erstellung der DSFA muss sich das datenbe-

arbeitende öffentliche Organ mit den eigenen Datenbearbeitungen und deren Risikopotenzial intensiv befassen. Dies schärft den Blick für datenschutzrechtliche Aspekte. Entscheidend ist auch, dass dies im Vorfeld einer Datenbearbeitung geschieht. Denn in diesem Zeitpunkt ist der Handlungsspielraum grösser. Das Thema Privatsphäre muss zu einem sehr frühen Zeitpunkt behandelt werden und den ganzen Prozess begleiten.

# 4 Ausblick

## 4.1 Leistungsvereinbarung mit Katholischem Konfessionsteil

Im Jahr 2020 wird die FDS für den Katholischen Konfessionsteil die Aufgabe der Datenschutzfachstelle wahrnehmen. Dafür ist ein Pensum von 10 Stellenprozenten vorgesehen, das der Katholische Konfessionsteil vollumfänglich vergütet. Die Modalitäten sind in einer Leistungsvereinbarung geregelt.

## 4.2 Revidiertes Datenschutzgesetz

Auch im 2020 werden die neuen Instrumente des revidierten DSG die FDS beschäftigen. Einerseits gibt es offene Fragen, die Praxis und Rechtsprechung klären werden (siehe dazu Abschnitt 1.1). Es wird sich auch zeigen, wie sich die Anzahl der Vorabkonsultationen entwickelt. Die Entwicklung dieses Instruments hängt auch mit der Ressourcenfrage zusammen. Dies deshalb, weil es sich um ein bedeutendes Instrument handelt, bei dem komplexe Sachverhalte beurteilt werden müssen und die Zusammenarbeit mit anderen Stellen erforderlich ist. Interessant wird auch sein, wie sich die neuen Instrumente bei den Gemeindefachstellen auswirken. Im Zusammenhang mit der Zusammenarbeit bei den Vorabkonsultationen mit dem DIP stellt sich die Frage nach fachstellen-internem IT-Know-how. Die Zusammenarbeit mit dem DIP ist sehr gut. Allerdings verfügt er nicht über die Unabhängigkeit, welche die FDS hat. National zeigt sich denn auch die Tendenz, dass nicht nur in den «grossen Datenschutz-Kantonen» wie Zürich und Basel, sondern vermehrt auch in den «mittelgrossen Datenschutz-Kantone» wie Aargau oder Solothurn die Datenschutzstellen eigene IT-Fachleute rekrutieren.

## 4.3 Prüfprogramm 2020

Die FDS legt für das Jahr 2020 unten stehendes Prüfprogramm fest:

1. Arbeitsbesuch bei einer Gemeindefachstelle für Datenschutz
2. Applikation E-Personaldossier
3. Applikation Jagd und Fischerei (EFJ)
4. Schengenkontrolle beim Migrationsamt

# 5 Antrag

Wir beantragen Ihnen, Herr Präsident, sehr geehrte Damen und Herren, auf den Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2019 einzutreten.

Kantonale Fachstelle für Datenschutz

Corinne Suter Hellstern, Leiterin