



Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2021



1	Zusammenfassung	4
2	Schwerpunkte	6
2.1	E-Government	6
2.2	Risikoanalysen	7
3	Prüftätigkeit	8
3.1	Applikation Jagd und Fischerei	8
3.2	Chatbot Handelsregisteramt	8
3.3	Kantonale Einwohnerdatenplattform	9
3.4	Lernfördersysteme	9
3.5	Schengen-Kontrolle beim Migrationsamt	9
4	Aufsicht und Beratung Gemeindefachstellen	10
4.1	Arbeitsbesuch	10
4.2	Zugriffe auf kantonale Einwohnerdatenplattform	10
4.3	Erfahrungsaustausch	10
5	Rechtsetzung	11
5.1	Vorabkonsultationen	11
5.1.1	<i>Digitaler Posteingang in Personalsachen</i>	11
5.1.2	<i>Electronic Monitoring</i>	11
5.1.3	<i>PIAZO / PICAR</i>	12
5.1.4	<i>Universitätsgesetz</i>	12
5.1.5	<i>Gesetz über Videoüberwachung, automatische Fahrzeugfahndung und Polizeigesetz</i>	13
5.1.6	<i>Diverses</i>	13
5.2	Ausserkantonale Erlasse	14
6	Einzelanfragen	15
6.1	Applikationen für Online-Unterricht	15
6.2	Darmkrebs-Screening	15
6.3	Online-Beratungen	15
6.4	Wir-impfen.ch	16
6.5	Mediananfragen	16

7	Verzeichnis der Bearbeitungstätigkeit	17
8	Zusammenarbeit und Sensibilisierung	18
9	Personelles und Ressourcen	19
10	Prüfprogramm 2022	21
11	Antrag	21
12	Anhang – Zahlen	22



E-Government, digitaler Posteingang in Personalsachen, Applikationen für Online-Unterricht – auch im Berichtsjahr beschäftigte sich die Fachstelle für Datenschutz (FDS) mit vielfältigen Themen. Bei E-Government, der Digitalisierung verschiedener Services der Behörden, sind Datenschutz und Datensicherheit wichtige Themen. Die FDS äusserte sich zum Personenregister und zu den Datenaustausch-Vereinbarungen.

Seit rund zwei Jahren ist das revidierte kantonale Datenschutzgesetz in Kraft. Damit wurden die Datenschutz-Folgenabschätzung und die Meldepflicht für Datenschutzverletzungen eingeführt. Die Datenschutz-Folgenabschätzung ist eine Risikoanalyse. Das öffentliche Organ muss sie vor der Bearbeitung von Personendaten mit einem möglicherweise hohen Risiko erstellen. Die FDS geht davon aus, dass es heute kaum mehr Projekte gibt, bei denen auf eine solche Abschätzung verzichtet werden kann. Es gingen einige Anfragen zu diesem Thema ein. Stellt das öffentliche Organ ein hohes Risiko für die Grundrechte fest, muss es das Vorhaben der FDS zur Vorabkonsultation vorlegen. Diese hat definiert, in welchen Fällen stets, ohne dass ein hohes Risiko vom öffentlichen Organ festgestellt wird, eine Vorabkonsultation erforderlich ist. (Noch) kein grosses Thema war im Jahr 2021 die Meldepflicht bei Verletzungen der Datensicherheit.

Die FDS prüfte eine Applikation im Bereich Jagd und Fischerei, die administrativen Abläufen dient. Zwar werden nicht in grossem Umfang sensible Personendaten bearbeitet, es können jedoch zahlreiche Stellen darauf zugreifen. Ausserdem handelt es sich um eine Auftragsdatenbearbeitung. Punkte, die aus datenschutzrechtlicher Sicht immer heikel sind. Empfehlungen machte die FDS zur Klassifikation, Aufbewahrungsdauer und Stellvertretung. Zudem prüfte sie den Chatbot beim Handelsregisteramt. Damit sollen Standardanfragen automatisiert und Bestellungen im Handelsregister ermöglicht werden. Die Umsetzung machte einen guten Eindruck, beim momentanen Einsatz werden nur marginal Personendaten bearbeitet. Wie bei allen neuen Technologien, die sich rasch und stark ändern können, muss die weitere Entwicklung aber im Auge behalten werden.

Den jährlichen Arbeitsbesuch machte die FDS bei der Gemeindefachstelle Oberuzwil. Wie bereits in früheren Jahren war vor allem die Unabhängigkeit Thema. Die Fachstellenleitung ist sowohl datenbearbeitende Behörde als auch Datenschutz-Aufsichtsstelle. Die FDS steht einer solchen Kombination kritisch gegenüber, weil damit die heutigen Anforderungen an die Unabhängigkeit nicht erfüllt werden können. Zudem erachtet die FDS 20 Stellenprozente mit Blick auf die gesetzlich vorgesehene Aufgabenerfüllung als zu gering. Dessen ungeachtet erfüllt die Fachstellenleitung die Aufgaben gut.

Die FDS bearbeitete einige Vorabkonsultationen in der Rechtsetzung: digitaler Posteingang in Personalsachen, Electronic Monitoring, interkantonaler Datenaustausch bei serieller Kriminalität und Universitätsgesetz. Zudem war das Gesetz über Videoüberwachung Thema, dazu läuft derzeit die Vernehmlassung.

Bei den Einzelanfragen waren Online-Beratungen ein Thema und – wie bereits im Vorjahr – Applikationen für den Online-Unterricht. Aufgrund des Grundsatzes der Verhältnismässigkeit muss stets die datensparsamste Variante gewählt werden. Zudem gab es einige vorwiegend technische Fragen zur Webseite wir-impfen.ch. Für die Klärung dieser Fragen musste die FDS einen externen Sicherheitsexperten beiziehen, da sie selbst über keine Fachperson für Informationssicherheit verfügt.

Die Anzahl der Geschäftseingänge bewegte sich auch im Berichtsjahr auf einem hohen Niveau. Wie sich seit einiger Zeit abzeichnet, ist für die Beanspruchung der FDS aber nicht mehr hauptsächlich die Anzahl, sondern die Komplexität der Geschäfte massgebend. Auch bestätigt sich der Trend weg von einfach zu beantwortenden Einzelanfragen hin zu komplexen Vorlagen mit teilweise grossen politischen und gesellschaftlichen Auswirkungen.

Die Digitalisierung führt zu zahlreichen komplexen Anfragen. Dabei stellen sich nicht nur juristische Fragen, sondern auch Fragen der Datensicherheit. Um die gesetzlichen Aufgaben unabhängig wahrnehmen zu können, benötigt die Fachstelle für Datenschutz auch Know how in diesem anspruchsvollen technischen Bereich. Die FDS beantragt deshalb Ressourcen für die Schaffung einer Stelle im Bereich Informationssicherheit.

Frau Präsidentin
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^{2,3}. Der vorliegende Bericht gibt Rechenschaft über die Tätigkeit der FDS im Jahr 2021.

1

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

2

sGS 140.1.

3

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

2.1 E-Government

E-Government, die Digitalisierung verschiedener Services der Behörden, war im Berichtsjahr ein wichtiges Thema. Ziel des Datenschutzes ist, die Privatsphäre betroffener Personen zu schützen. Datensparsamkeit ist ein wichtiger Grundsatz. Bei der Digitalisierung hingegen werden sehr viele auch sensible Daten bearbeitet, und das digital. Die digitale Bearbeitung birgt höhere Risiken für die Grundrechte der betroffenen Personen als die Bearbeitung auf Papier. Zudem sind die Projekte häufig sehr komplex mit vielen verschiedenen Anspruchsgruppen. Datenschutz ist bei E-Government deshalb ein wichtiges Thema, v.a. auch, um das nötige Vertrauen bei Bürgerinnen und Bürgern zu schaffen. Als Grundlage von E-Government ist der Aufbau eines zentralen Personenregisters vorgesehen. Ausgangspunkt ist das bereits heute existierende kantonale Einwohnerregister. Dieses soll mit Daten von gemeldeten Personen und Personen, die sich im Kanton aufhalten, beispielsweise Grenzgängerinnen und Grenzgängern, ergänzt werden. Derzeit werden diese Daten im ZEMIS-Register beim Migrationsamt geführt. Zudem soll es um alle Personen mit einem steuerrechtlichen Bezug zum Kanton erweitert werden. Wichtig ist, die Frage der Rechtsgrundlage im Auge zu behalten: Beim Gesetz über E-Government⁴ handelt es sich um einen Rahmenerlass, er genügt als Rechtsgrundlage nicht. Das Gesetz über Niederlassung und Aufenthalt regelt aktuell nur den Betrieb der kantonalen Einwohnerdatenplattform (KEWR) und nicht die Erweiterung zu einem Personenregister.

Ein weiteres Thema waren die Datenaustausch-Vereinbarungen, die zwischen den öffentlichen Organen abgeschlossen werden. Damit werden die Modalitäten des Datenaustausches geregelt. Die FDS hielt fest, dass diese Vereinbarungen für den Austausch von Personendaten nur deklaratorischen Charakter haben, massgebend ist stets das Datenschutzgesetz.

Wichtig bei E-Government-Projekten ist die Information und Sensibilisierung der Projektleitenden: Sie müssen darauf hingewiesen werden, dass bei einem möglichen hohen Risiko für die Grundrechte der betroffenen Personen eine Datenschutz-Folgenabschätzung erforderlich ist, der allenfalls eine Vorabkonsultation folgt. Die FDS geht davon aus, dass eine Datenschutz-Folgenabschätzung bei E-Government-Projekten in den meisten Fällen nötig ist.



4
sGS 142.3.

2.2 Risikoanalysen

Die Datenschutz-Folgenabschätzung wurde mit der Revision des DSG vor gut zwei Jahren eingeführt: Dabei handelt es sich um eine Risikoanalyse einer Behörde. Sie ist Pflicht, wenn eine Datenbearbeitung ein hohes Risiko für die Grundrechte der Bürgerinnen und Bürger mit sich bringen kann. Heute dürfte dies auf die meisten Vorhaben zutreffen. Das bedeutet, dass bei den meisten Vorhaben eine Datenschutz-Folgenabschätzung gesetzliche Pflicht ist. Die FDS erachtet das Instrument als sehr wichtig: Die öffentlichen Organe werden damit bezüglich der Datenschutzrisiken eines Vorhabens sensibilisiert und können rechtzeitig entsprechende Massnahmen ergreifen. Die Datenschutz-Folgenabschätzung stärkt auch die (Eigen)Verantwortung, die bei jeder Datenbearbeitung beim öffentlichen Organ verbleibt. Die Datenschutz-Folgenabschätzung muss vor einer Datenbearbeitung gemacht werden. Bei ihren Kontrollen wird die FDS prüfen, ob eine Datenschutz-Folgenabschätzung gemacht wurde.

Stellt das öffentliche Organ als Ergebnis der Datenschutz-Folgenabschätzung ein hohes Risiko fest und kann keine Massnahmen treffen, die das Risiko verringern, muss das Vorhaben der FDS zur Vorabkonsultation vorgelegt werden. Gewisse Vorhaben wie Videoüberwachung oder Gesichtserkennung müssen in jedem Fall zur Vorabkonsultation vorgelegt werden. Die FDS hat in ihrem Merkblatt⁵ definiert, welche Vorhaben darunterfallen.

5

[Merkblatt Vorabkonsultation](#)

Bei der Rechtsetzung gab es einige Vorabkonsultationen (siehe dazu Ziff. 5 dieses Berichts). Das war zu erwarten, muss der FDS doch jedes Rechtsetzungsvorhaben, das datenschutzrechtlich relevant ist, vorgelegt werden. Zudem besteht mit den Vernehmlassungen und Mitberichten bereits seit langem ein eingespieltes Instrument. Für die öffentlichen Organe ist es nichts Neues, die Stellungnahmen betroffener Stellen einzuholen und sie tun es routinemässig. Etwas anders sieht es bei Projekten ausserhalb der Rechtsetzung aus. Der FDS stellt sich die Frage, ob alle Vorhaben zur Vorabkonsultation kommen, bei denen das Gesetz dies vorsieht. Die FDS hat zur digitalen Unterschrift bei der Kapo eine Vorabkonsultation durchgeführt, ein paar weitere Vorhaben sind angekündigt. Die FDS wird mit ständiger Information und Sensibilisierung weiter daran arbeiten, dass die Instrumente zum Standard werden.

Die Meldepflicht von Datenschutzverletzungen war auch im Berichtsjahr kaum ein Thema. Eine Meldung betraf einen Trojaner; die FDS verwies an die zuständige Stelle, da sie über keine eigenen Ressourcen in der IT-Sicherheit verfügt. Angesichts der zunehmenden Datenschutz- und Sicherheitsverletzungen ist davon auszugehen, dass inskünftig mehr Fälle gemeldet werden.

3.1 Applikation Jagd und Fischerei

eFJ2 ist eine Applikation für die Abwicklung administrativer Abläufe bei Jagd und Fischerei. Mehrere Kantone nutzen diese Applikation. Die Ergebnisse der Prüfung wurden nach Rücksprache mit der geprüften Stelle den Datenschutzbeauftragten der beteiligten Kantone zugestellt.

In der Applikation werden zwar nicht in grossem Umfang sensible Personendaten bearbeitet, es können jedoch zahlreiche Stellen auf die Daten zugreifen. Ausserdem handelt es sich um eine Auftragsdatenbearbeitung. Der Datenschutz ist deshalb auch bei eFJ2 ein wichtiges Thema. eFJ2 hat ihre Anfänge in einer Zeit, als IT-Sicherheit und Datenschutz nicht standardmässig berücksichtigt wurden: Die Verträge enthalten keine diesbezügliche Bestimmung, ebenso wenig waren Löschung bzw. Vernichtung der Personendaten ein Thema. Da zudem mehrere Kantone beteiligt sind, bedürfen wesentliche Änderungen der Zustimmung aller Kantone. Das ist nicht die einfachste Ausgangsposition für eine stringente Umsetzung der datenschutzrechtlichen Vorgaben. Angesichts dessen macht die Umsetzung des Datenschutzes einen passablen Eindruck: Auch wenn die Datenschutz-Themen nicht zuoberst auf der Prioritätenliste stehen, ist den Mitarbeitenden dieses Thema bewusst und sie handeln danach. Im Einzelnen empfahl die FDS insbesondere folgende Massnahmen: Die Applikation muss als «geheim» klassifiziert werden, weil auch besonders schützenswerte Personendaten bearbeitet werden. Aus der Applikation ist ersichtlich, ob eine Person für die Ausübung von Jagd oder Fischerei gesperrt ist und aus welchem Grund (diese Angabe wird in Kategorien angegeben). Die Dokumentation dazu ist nicht ersichtlich. Aber selbst wenn der Grund nicht angegeben wird, handelt es sich bei der Tatsache der Sperrung um eine Bearbeitung besonders schützenswerter Personendaten. Die in eFJ2 bearbeiteten Personendaten werden dauernd aufbewahrt, bei Todesfall werden die Personendaten deaktiviert. Die FDS empfahl, eine Aufbewahrungsdauer festzulegen. Eine längere Aufbewahrungsfrist ist vertretbar, die ständige Aufbewahrung hingegen widerspricht dem DSG. Zudem muss die Stellvertretung geregelt werden: Ebenso wenig wie ein längerer technischer Ausfall des Systems toleriert werden kann, ist dies auch bei einem längeren personellen Ausfall gegeben. Weitere Empfehlungen betrafen Anpassungen der AGB zum Webshop, den Vertrag mit dem Auftragsdatenbearbeiter und den Prozess zur Meldung von Verletzungen der Datensicherheit.

3.2 Chatbot Handelsregisteramt

Die FDS prüfte den Chatbot des Handelsregisteramts. Der Chatbot ist seit Anfang Juni 2021 bis Ende 2023 als Pilot in Betrieb, danach wird über eine Weiterführung entschieden. Hauptziel ist, die Bearbeitung von Standardanfragen zu automatisieren und Bestellungen im Handelsregister zu ermöglichen. Beim Chatbot handelt es sich um eine Wissensdatenbank und keinen Online-Schalter, bei dem Dokumente bearbeitet werden. Die Umsetzung macht einen guten Eindruck: Die Prüfung ergab, dass beim derzeitigen Einsatz des Chatbot nur marginal Personendaten bearbeitet werden. Datenschutzthemen wurden sorgfältig abgeklärt und bereits in der Anfangsphase ein Sicherheitsaudit gemacht. Die FDS begrüsst zudem sehr, dass neue Technologien datensparsam eingesetzt werden. Die Projektverantwortlichen haben erkannt, dass es wichtig ist – gerade

bei neuen Technologien – Vertrauen bei der Bevölkerung zu schaffen. Wie bei allen neuen Technologien, die sich rasch und stark ändern können, muss die weitere Entwicklung stets im Auge behalten werden. Es muss geklärt werden, inwiefern Personendaten tangiert sind und dies ein Risiko für die betroffenen Personen darstellt.

3.3 Kantonale Einwohnerdatenplattform

Die kantonale Einwohnerdatenplattform beinhaltet Daten der Einwohnerinnen und Einwohner des Kantons St.Gallen. Der Kanton betreibt die Plattform, die Gemeinden liefern die Einwohnerdaten. Zugriff haben vor allem kantonale Stellen, welche die Daten für ihre Aufgabenerfüllung benötigen. Die revidierte Verordnung über die kantonale Einwohnerdatenplattform⁶ ist am 7. Januar 2020 in Vollzug getreten. Seitdem nimmt die FDS vorgängig keine Stellung mehr zu den Anträgen für die Zugriffsberechtigungen. Die Ermächtigung, wer auf welche Datenfelder Zugriff hat, erfolgt neu über das jeweils oberste Leitungsorgan. Der Dienst für Informatikplanung (DIP) schaltet auf Gesuch hin die Zugriffe frei. Deshalb sah die FDS in ihrem Tätigkeitsbericht 2019 vor, stichprobenweise die Zugriffsberechtigungen zu prüfen. Ziel ist dabei die Prüfung, ob das Zugriffskonzept eingehalten wird. Im Berichtsjahr wurden zwei Dienststellen der Staatskanzlei geprüft. Weiter wurde die Prüfung beim Amt für Soziales sowie bei drei Stellen des Gesundheitsdepartements gemacht. Die Prüfungen bei den beiden Dienststellen der Staatskanzlei sind abgeschlossen. Die Zugriffe sind aus datenschutzrechtlicher Sicht plausibel, Empfehlungen waren nicht notwendig. Die Prüfung der anderen Stellen ist derzeit noch hängig.

6

sGS 453.11.

3.4 Lernfördersysteme

Die zuständige Stelle bat um eine Verschiebung der Prüfung: Einerseits wechselte die leitende Person, andererseits wurden die Lernfördersysteme einem Sicherheitsaudit unterzogen, das bis Ende des Berichtsjahrs dauerte. Es ist sinnvoll, diese Ergebnisse abzuwarten und danach die datenschutzrechtliche Prüfung zu machen.

3.5 Schengen-Kontrolle beim Migrationsamt

Der Fragebogen für die Schengen-Kontrolle beim Migrationsamt wurde Ende des Berichtsjahres verschickt. Vorgesehen ist eine zweistufige Kontrolle: In einem ersten Schritt wurde ein Fragebogen zu organisatorischen Themen verschickt. In einem zweiten Teil sollen die Zugriffe der Mitarbeitenden auf das Schengener-Informationssystem überprüft werden (Kontrolle der Logfiles⁷). Zudem werden die Mitarbeitenden bezüglich ihrem Umgang mit dem Schengener-Informationssystem befragt.

7

Automatisch geführtes Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem (Quelle: Wikipedia, Stand Januar 2022).

4.1 Arbeitsbesuch

Die FDS machte zusammen mit dem Leiter Informationssicherheit des DIP einen Arbeitsbesuch bei der Gemeindefachstelle für Datenschutz Oberuzwil. Hauptthema war die Unabhängigkeit: Die leitende Person ist sowohl Leiterin verschiedener Ämter und Ressorts in der Gemeinde als auch Leiterin der Gemeindefachstelle für Datenschutz. Als Leiterin der Gemeindefachstelle für Datenschutz ist sie Datenschutzfachstelle verschiedener Gemeinden. Nach der Rechtsprechung ist die erforderliche völlige Unabhängigkeit nicht gegeben, wenn neben den Aufgaben im Datenschutz der Datenschutzstelle weitere Aufgaben übertragen werden. Die Unabhängigkeit war deshalb bereits im Jahr 2014 Thema. Die Gemeinde setzte darauf einige Massnahmen zur Verbesserung um. Seitdem sind die Anforderungen an die Unabhängigkeit weiter gestiegen. Auch der Stellenwert des Datenschutzes allgemein hat sich gegenüber früher deutlich erhöht. Zudem erschwert eine solche Organisation die Wahrnehmung der Datenschutzaufgaben, beispielsweise wenn Massnahmen getroffen werden müssen. Die FDS erachtet die Ausgestaltung der Stelle deshalb als nicht zufriedenstellend und hat angeregt, nach einer anderen organisatorischen Lösung zu suchen.

Dessen ungeachtet erfüllt die Stellenleiterin ihre Aufgabe angesichts der Rahmenbedingungen gut: Sie bearbeitet die Anfragen rasch und gewissenhaft und arbeitet gut mit den anderen Datenschutzfachstellen zusammen. Auch ihre Erfahrung kommt ihr zugute. Die ihr zur Verfügung stehenden 20 Stellenprozente sind allerdings zu wenig: Damit können die Anfragen beantwortet, aber keine Kontrollen durchgeführt werden. Für diese Funktion müssen mehr Stellenprozente zur Verfügung stehen, damit die gesetzlich vorgesehenen Aufgaben erfüllt werden können.

4.2 Zugriffe auf kantonale Einwohnerdatenplattform

In einem Fall zeigte sich, dass mehrere Stellen einer Gemeinde nicht nur auf die eigenen Einwohnerdaten, sondern auf die Daten sämtlicher Einwohnerinnen und Einwohner des Kantons Zugriff hatten. Es war nicht ersichtlich, welchem Zweck dies diente. Die FDS informierte die zuständige Gemeindefachstelle, die entsprechende Schritte einleitete, um den Zugriff zu unterbinden. Die neue Regelung, wonach die obersten leitenden Organe festlegen, wer Zugriff hat, stärkt die Eigenverantwortung der entsprechenden Stelle. Sie muss aber auch wahrgenommen werden.

4.3 Erfahrungsaustausch

Am Austausch mit den Gemeindefachstellen ging es um die Themen E-Government und Personenregister. Die FDS pflegt gemeinsam mit der Gemeindefachstelle der Stadt St.Gallen einen regelmässigen Austausch mit E-Government St.Gallen digital. Weitere Themen waren die Datenschutz-Folgenabschätzung und Vorabkonsultation. Beides ist bei den Gemeinden offenbar nach wie vor zu wenig bekannt und eine weitere Sensibilisierung angezeigt.

5.1 Vorabkonsultationen

5.1.1 Digitaler Posteingang in Personalsachen

Nachdem die Staatskanzlei die «digitale Postbearbeitung» im Vorjahr einführt, sollte nun der digitale Posteingang in Personalsachen eingeführt werden: Die eingehenden postalischen Sendungen, die Personelles betreffen, sollten zentral digitalisiert werden. Bei Personalangelegenheiten handelt es sich um besonders schützenswerte Personendaten. Sowohl Personalgesetz als auch Gesetz über die Archivierung sehen vor, dass zwecks Digitalisierung die mit dieser Aufgabe betrauten Personen auch besonders schützenswerte Personendaten bearbeiten können, sofern dies für die Aufgabenerfüllung unentbehrlich ist. Es stellte sich die Frage, wie unentbehrlich es ist, dass die Post nicht beim jeweiligen Personaldienst selbst, sondern zentral geöffnet und digitalisiert wird. Aus Sicht der FDS ist die Unentbehrlichkeit bei weiter Auslegung der Bestimmung gegeben. Die zentrale Öffnung und Digitalisierung hat den Vorteil, dass weniger Personen involviert und zudem räumlich und personell weiter weg sind von der Stelle, für welche sie die Post öffnen. Ausserdem ergibt sich eine gewisse Professionalisierung. Die Mitarbeitenden müssen aber vorgängig über die neue Organisation informiert werden. Zudem muss ihnen mitgeteilt werden, dass eine Öffnung durch die zentrale Poststelle verhindert werden kann, wenn man den Brief als vertraulich/persönlich adressiert.

5.1.2 Electronic Monitoring

Das Bundesrecht sieht mit Art. 28c des schweizerischen Zivilgesetzbuches⁸ neu vor, dass als zivilrechtliche Massnahme zum Schutz gewaltbetroffener Personen ein Electronic Monitoring angeordnet werden kann (Rayonverbot). Die Kantone setzen dies um. Aufgrund der zeitlichen Dringlichkeit wurde entschieden, die Umsetzung als Pilotversuch nach dem DSG⁹ zu lancieren. Dass das Electronic Monitoring mittels Pilotversuch geregelt werden sollte, lag für die FDS nicht auf der Hand, zumal nicht alle gesetzlichen Voraussetzungen erfüllt waren. So wurden beispielsweise die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen nicht näher definiert. Es stellte sich zudem die Frage, weshalb die Verordnung nicht als reguläre Verordnung erlassen wurde.

8

SR 210.

9

Art. 16a f. DSG.



Die FDS hielt allgemein zum Pilotversuch, der zum ersten Mal angewendet wurde, Folgendes fest: Bei der Bestimmung zum Pilotversuch geht es um eine «experimentelle Gesetzgebung». Dabei kann die Regierung vor Erlass eines Gesetzes die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen im Pilotversuch unter bestimmten Voraussetzungen bewilligen, nachdem sie die Stellungnahme der FDS dazu eingeholt hat. Die Bestimmung dient nicht dazu, eine schnelle vorübergehende Regelung zu erlauben. Sondern sie ist dafür vorgesehen, dass bei oft schnellem technologischem Fortschritt und dem langwierigen Gesetzgebungsprozess ab Beginn der Datenbearbeitung eine gesetzliche Grundlage vorhanden ist. Grundlage jedes staatlichen Handelns ist bekanntlich das Recht. Bekannter Regelungsbedarf darf nicht mit der Regelung als Pilotversuch vermieden werden. Auch darf das öffentliche Organ nicht weniger strenge Bestimmungen erlassen, als nötig und bekannt ist. Das Instrument des Pilotversuchs darf nicht dazu führen, dass die öffentlichen Organe zukünftig eine grosszügige Auslegung der Voraussetzungen von Art. 16a DSG vornehmen, um mit weniger strengen Bestimmungen arbeiten zu können. Dies würde zu einer unzulässigen Aushöhlung des Datenschutzes führen. Für einen Pilotversuch müssen deshalb strenge Anforderungen gelten.

5.1.3 PIAZO / PICAR

Die Ostschweizer Polizeibehörden möchten eine neue Datenbank für den interkantonalen Datenaustausch bei serieller Kriminalität nutzen. Derzeit fehlen dafür die gesetzlichen Grundlagen. Deshalb soll der Datenaustausch in einer interkantonalen bzw. interbehördlichen Vereinbarung geregelt werden. Die Projektleitung, die bei der Kapo St.Gallen liegt, lud die FDS zur Vorabkonsultation ein. Nach Ansicht der FDS müssen der Zweck präziser formuliert und die serielle Kriminalität definiert werden. Zudem muss klar festgehalten werden, welche Delikte in der Datenbank aufgenommen werden und wer welche Daten eingeben kann. Die Löschrufen müssen geregelt werden, wobei kürzere Löschrufen in kantonalen Gesetzen vorbehalten bleiben. Weil alle Ostschweizer Kantone betroffen waren, bezog die FDS auch die Stellungnahmen der anderen Datenschutzbeauftragten in ihre Vorabkonsultation ein. So konnten sie sich einerseits zu einem früheren Zeitpunkt äussern und andererseits entsteht eine gewisse Sicherheit, dass nicht zu einem späten Zeitpunkt noch völlig neue Aspekte berücksichtigt werden müssen.

5.1.4 Universitätsgesetz

Beim Universitätsgesetz thematisierte die FDS die sehr offen formulierten Datenschutzbestimmungen. Sie empfahl eine Konkretisierung und stärkere Bindung an den Zweck der Bearbeitung. Zudem erachtete sie die Datenbekanntgabe als zu weitgehend.

5.1.5 Gesetz über Videoüberwachung, automatische Fahrzeugfahndung und Polizeigesetz

Ebenfalls im Berichtsjahr wurde die FDS zur Vorabkonsultation zu den oben erwähnten Geschäften eingeladen. Die Vernehmlassung zu diesen Vorhaben läuft derzeit, auch die FDS wird dazu nochmals eine Stellungnahme abgeben. Im Folgenden wird deshalb nur in allgemeiner Form auf die gesetzliche Grundlage für die Videoüberwachung eingegangen. Über diese Thematik hat die FDS in vergangenen Jahren mehrmals berichtet.

Die FDS begrüsst die Schaffung einer Grundlage für die Videoüberwachung in einem formellen Gesetz. Als einer der wenigen Kantone verfügt der Kanton St.Gallen bisher nicht über eine Regelung für kantonale Organe. Frühere Anfragen bei der FDS und eine im Jahr 2018 durchgeführte Befragung bei kantonalen Schulen zeigten, dass auch kantonale Organe Videoüberwachung durchführen. Die FDS wies mehrmals in ihren Tätigkeitsberichten¹⁰ darauf hin, dass es für die Videoüberwachung einer Grundlage in einem formellen Gesetz bedürfe.

Jedem Menschen steht das Recht zu, sich in der Öffentlichkeit bewegen zu können, ohne dass sein Verhalten durch eine Kamera aufgezeichnet wird. Bei der Videoüberwachung werden unverdächtige Menschen mit ihren individuellen Verhaltensweisen Gegenstand einer staatlichen Beobachtung oder Aufzeichnung. Die Videoüberwachung macht das Verhalten transparent und kontrollierbar. Die Gefahr für den demokratischen und freiheitlichen Rechtsstaat besteht weniger in der einzelnen Videoüberwachung, als vielmehr in ihrer grossen Vielzahl und den umfassenden Einsatzgebieten. Der schleichende Übergang zu einem Überwachungsstaat und damit einer ernsthaften Gefahr für die Freiheit und Privatsphäre muss immer im Auge behalten werden.

Deshalb sollte ein Register oder eine Karte geführt werden, auf der die Videoüberwachungen im Gesamtbild ersichtlich sind. Zudem muss nach einer gewissen Zeit eine Evaluation erfolgen, ob die Videoüberwachung ihr Ziel erreicht hat. Stets muss auch der Grundsatz der Verhältnismässigkeit, die Datenvermeidung und Datensparsamkeit, beachtet werden.

Damit eine gesetzliche Grundlage genügt, müssen im formellen Gesetz die Orte und Voraussetzungen der Videoüberwachung geregelt werden, zudem der Bearbeitungszweck, die zur Datenbearbeitung befugten Stellen, die technischen Mittel und Einsatzformen, Auswertung, Bekanntgabe und Aufbewahrung sowie die Schutzvorkehrungen.¹¹ Der Bearbeitungszweck muss im formellen Gesetz eindeutig und präzise festgelegt werden.

5.1.6 Diverses

Im Weiteren hat die FDS zu folgenden kantonalen Vorhaben Stellung genommen:

- Einführungsgesetzgebung zum eidgenössischen Waldgesetz
- Ausländerdatenbank beim Migrationsamt

10

Vgl. Tätigkeitsberichte 2017 S. 3, 2016 S. 3, 2015 S. 7 und 2014 S. 6 f.

11

Vgl. Müller, Lucien, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, Dike Verlag Zürich / St.Gallen 2011, S. 210 ff.

5.2 Ausserkantonale Erlasse und Vorhaben

Die FDS nahm zu folgenden ausserkantonalen Erlassen und Vorhaben Stellung:

- Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus
- Plattform elektronische Kommunikation in der Justiz
- Schengen Evaluierung (Follow-up)
- Weiterentwicklungen des Schengen-Besitzstandes
- Verordnung zum Bundesgesetz über den Datenschutz
- Vorläuferstoffverordnung



6 Einzelanfragen

Wie in jedem Jahr bearbeitete die FDS zahlreiche Einzelanfragen. Es stellten sich Fragen zu Homeoffice, Lernfördersystemen, Microsoft 365 oder der Verwendung der AHV-Nummer. Im Folgenden wird ein Ausschnitt allgemein interessierender Themen aufgezeigt.

6.1 Applikationen für Online-Unterricht

Zu Beginn der Pandemie gab es viele Anfragen zum Online-Unterricht und zu Applikationen, die eingesetzt werden konnten. Das Bildungsdepartement (BLD) wählte bei den Kantons- und Berufsschulen einen in datenschutzrechtlicher Hinsicht begrüssenswerten Ansatz: Neue Applikationen wurden von einem IT-Ausschuss, bestehend aus Lehrpersonen, vorgängig geprüft. Bei Bedarf wurde die FDS beigezogen. Wurde die Applikation als mit dem Datenschutz kompatibel beurteilt, wurde sie auf die Liste des BLD gesetzt. Eine Anfrage betraf die Verwendung eines Lernförderprogramms; dieses konnte sowohl anonym als auch mit Klarname verwendet werden. Der Anbieter beantragte, dass das Lernförderprogramm mit Klarname verwendet werde. Aus datenschutzrechtlicher Sicht ist dies abzulehnen: Aus dem Grundsatz der Verhältnismässigkeit lässt sich die Datensparsamkeit ableiten. Danach sollen so viele Personendaten wie nötig und so wenig wie möglich bearbeitet werden. Sind also beide Anwendungen möglich, soll die anonyme Variante gewählt werden.

6.2 Darmkrebs-Screening

Der Kanton St.Gallen beabsichtigt, ein Früherkennungsprogramm gegen Darmkrebs einzuführen. Bereits heute gibt es das Früherkennungsprogramm gegen Brustkrebs. Für dieses gibt es eine explizite gesetzliche Grundlage. Eine solche fehlt beim Darmkrebs-screening derzeit und sie muss noch geschaffen werden.

6.3 Online-Beratungen

Beratungen durften wegen der Pandemie teilweise nicht mehr persönlich durchgeführt werden, die öffentlichen Organe mussten aber dennoch ihre gesetzlichen Aufgaben erfüllen. Deshalb stellte sich seit Beginn der Pandemie die Frage, wie Online-Beratungen bzw. Videokonferenzen kompatibel mit dem Datenschutzrecht durchgeführt werden können. Nebst der Frage nach der Rechtsgrundlage ist bei einem Eingriff in das Grundrecht auf Privatsphäre immer auch die Verhältnismässigkeit zu beurteilen. Braucht es für die Beratung eine Videokonferenz oder genügt der telefonische Kontakt? Es muss immer die datensparsamste Variante gewählt werden. Dies gilt besonders für sehr sensible Beratungen etwa bei der Sozialhilfe oder Arbeitslosigkeit. Die betroffene Person sollte im Voraus über das gewählte Tool und allfällige datenschutzrechtliche Risiken informiert werden. Eine Aufzeichnung ist ohne informierte, ausdrückliche und freiwillige Einwilligung nicht zulässig. Zudem sind organisatorische und technische Massnahmen zu beachten, wie ein eingeschränktes Zugriffsrecht, eine End-to-end Verschlüsselung, keine Speicherung auf einem Server und es dürfen nur berechnigte Teilnehmende zugelassen sein. Das online durchgeführte Beratungsgespräch ist ein Ersatz für ein persönliches Beratungsgespräch und sollte nur in Ausnahmefällen eingesetzt werden.

6.4 wir-impfen.ch

Im Berichtsjahr gingen einige Anfragen im Zusammenhang mit der Webseite www.wir-impfen.ch ein. Es stellten sich Fragen im Zusammenhang mit der Registrierung, der Impfbestätigung, dem Speicherort, der Nutzung von Google Analytics und Amazon sowie den Löschmechanismen. Einige Anfragen, wie jene zu Zuständigkeit oder Nutzung von Google Analytics konnten geklärt werden, Google Analytics kommt nicht mehr zum Einsatz. Die noch offenen technischen Fragen liess die FDS durch eine externe Fachperson klären, da sie selbst über keine Fachperson für Informationssicherheit verfügt. Die Klärung wurde im Berichtsjahr noch nicht abgeschlossen.

6.5 Medienanfragen

Bei den Medienanfragen war – wie bereits im Vorjahr – die Gesichtserkennungssoftware bei der Polizei Thema, ausserdem der Zugriff auf Clearview (ebenfalls eine Gesichtserkennungssoftware), Fragen im Zusammenhang mit Corona und allgemeine Fragen zum revidierten Datenschutzgesetz.



7 Verzeichnis der Bearbeitungstätigkeit

Die Polizei muss ihre Datensammlungen neu – nach Anhörung der FDS – vom Sicherheits- und Justizdepartement genehmigen lassen.¹² Im Berichtsjahr hat die FDS erstmals zu den Datensammlungen der Polizei Stellung genommen. Die Führung der Datensammlungen erschien in den meisten Fällen plausibel. Kann die Polizei glaubhaft darlegen, dass sie die entsprechende Datensammlung für ihre Aufgabenerfüllung benötigt, darf deren Führung als rechtmässig angesehen werden, sofern kein rechtlicher Vorbehalt besteht. Die Verantwortung verbleibt bei der Polizei als datenbearbeitendes öffentliches Organ. Bei einzelnen Datensammlungen brachte die FDS Vorbehalte an, weil für sie beispielsweise nicht ersichtlich war, wozu die Datensammlung diene oder diese zu umfassend war. Die Stellungnahme ist anspruchsvoll, weil sie Wissen um Organisation, Aufgaben und Abläufe bei der Polizei erfordert. Zudem beansprucht sie viel Zeit, sind doch immer wieder Rückfragen nötig.

12

Art. 32 Polizeigesetz, sGS 451.1.

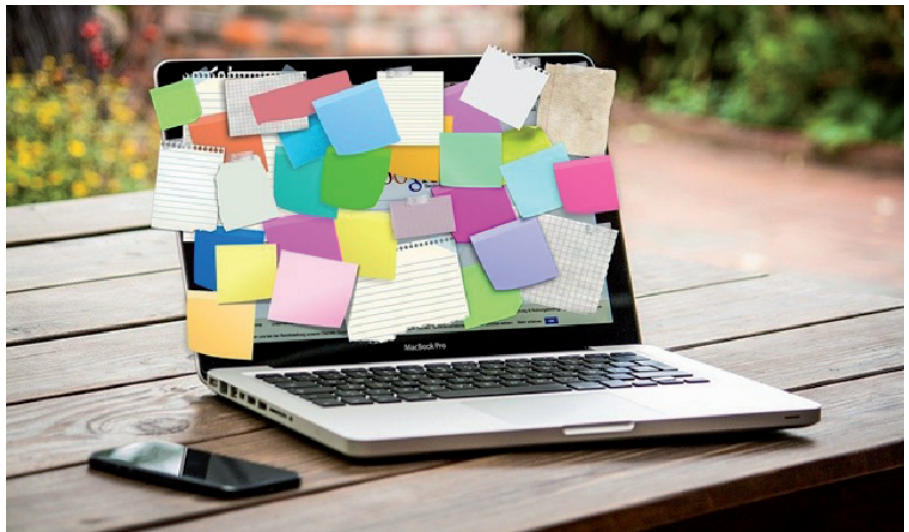


8 Zusammenarbeit und Sensibilisierung

Die FDS erachtet die Zusammenarbeit als sehr wichtig und pflegt regelmässige Kontakte insbesondere mit den Gemeindefachstellen für Datenschutz, aber auch mit den Ostschweizer Datenschutzbeauftragten, mit privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, und verschiedenen für den Datenschutz wichtigen Stellen des Kantons.

Die Datenschutzthemen sind je länger je mehr nicht auf den Kanton begrenzt, sondern es stellen sich häufig dieselben Fragen oder es werden gemeinsame Projekte geplant wie etwa PIAZO / PICAR in den Ostschweizer Kantonen. Die FDS fördert in ihrem Bereich die Zusammenarbeit und organisiert regelmässige Austausche mit den Gemeindefachstellen und den Ostschweizer Datenschutzbeauftragten. Der Austausch mit privatim findet vor allem über die Vorstandsarbeit statt.

Wie in jedem Jahr erstellte die FDS auch im Berichtsjahr eine Lerneinheit für das E-Learning «Informationssicherheit und Datenschutz». Thema war das Recht auf Vergessen und das Recht auf Erinnerung, die Aufbewahrung, Anbietepflicht und Vernichtung von Personendaten. Die FDS arbeitete dafür zusammen mit dem Staatsarchiv. Zudem erstellte sie ein Video für die Mitarbeitenden der kantonalen Verwaltung und verfasste Beiträge für verschiedene Medien.



Die FDS verfügte im Berichtsjahr bis Ende Oktober unverändert über 150 Stellenprozente. Der juristische Mitarbeiter reduzierte sein 40-Prozent-Pensum per Ende Oktober auf 10 Prozent, sein Nachfolger hat wiederum ein Pensum von 40 Prozent inne. Seit Anfang November verfügt die FDS über 160 Stellenprozente im juristischen Bereich. Wie bereits in den Vorjahren ist die Arbeitsbelastung hoch und verhartet seit einigen Jahren auf einem hohen Niveau. Bereits vor einiger Zeit zeichnete sich ab, dass für die Beanspruchung der FDS nicht mehr hauptsächlich die Anzahl, sondern die Komplexität der Geschäfte massgebend ist. Auch bestätigt sich der Trend weg von einfach zu beantwortenden Einzelanfragen hin zu komplexen Vorlagen mit teilweise grossen politischen und gesellschaftlichen Auswirkungen.

Mit E-Government soll die Digitalisierung gefördert werden, zahlreiche Stellen sehen Projekte vor. Der Datenschutz und die Datensicherheit spielen dabei eine grosse Rolle. Damit dürfte sich der Beratungs- und Kontrollaufwand weiter stark erhöhen. Die Digitalisierung führt aber nicht nur zu juristischen Fragen, sondern auch zu solchen der Datensicherheit. Die Bewältigung der Datenschutzthemen erfordert eine immer engere Zusammenarbeit dieser beiden Disziplinen. Die Prüfung der Angemessenheit von technischen und organisatorischen Massnahmen braucht Fachwissen im Bereich der Datensicherheit. Dieses ist zudem erforderlich für Kontrollen, Vorabkonsultationen (Prüfung von Schutzbedarfsanalysen, ISDS-Konzepte) und bei der Beratung zu Datenschutz-Folgenabschätzungen. Aber auch bei der Beratung in Einzelfällen und Stellungnahmen zu Rechtsetzungsvorhaben stellen sich häufig Fragen der Datensicherheit. Bei der Meldepflicht von Datenschutzverletzungen ist angesichts der allgemein zunehmenden Datenschutz- und Sicherheitsverletzungen anzunehmen, dass inskünftig mehr Meldungen bearbeitet werden. Auch die Erfüllung dieser Aufgabe braucht Fachwissen im Bereich der Datensicherheit.

Die FDS arbeitet seit ihrer Einsetzung im Jahr 2009 mit dem Leiter Informationssicherheit des DIP zusammen. Die Zusammenarbeit ist gut und konstruktiv. Der Leiter Informationssicherheit verfügt aber nicht über die Unabhängigkeit, welche die FDS hat. Die Anforderungen an die Unabhängigkeit der Datenschutzstellen sind von Gesetzes wegen sehr hoch und wurden stetig erhöht. Diese Unabhängigkeit ist unabdingbar, um die Aufgaben sowohl beim Datenschutz als auch bei der Datensicherheit im Sinn des DSG erfüllen zu können. Der Leiter Informationssicherheit verfügt zudem auch nur über beschränkte Ressourcen und ist anderweitig stark ausgelastet.

Damit eine Digitalisierungsstrategie gelingt, ist es unabdingbar, dass auch der Datenschutz gestärkt wird: Für jede Digitalisierung braucht es das Vertrauen der Bevölkerung. Und der Datenschutz ist ein wichtiges Element, um dieses Vertrauen zu gewinnen. Der FDS ist es ein Anliegen, kooperativ und auch in zeitlicher Hinsicht angemessen zu handeln. Dafür braucht es Fachstellen-internes IT-Know-how, damit die Themen rasch und unabhängig bearbeitet werden können. Es geht darum, pragmatische Lösungen zu erarbeiten, und dafür braucht es den ständigen Austausch von Recht und Informatik. Die Digitalisierung nimmt mehr und mehr Fahrt auf, daher ist jetzt der richtige Zeitpunkt zur Schaffung einer Stelle für Datensicherheit bei der FDS. Dies nicht zuletzt aufgrund der Tatsache, dass einige kantonale Stellen bereits angekündigt haben, umfassende Projekte zur Vorabkonsultation einzureichen. Wie bereits in den Vorjahren erwähnt¹³, verfügen andere Kantone mit vergleichbarer Grösse schon seit längerem über IT-Stellen. Die FDS wird daher einen entsprechenden Antrag im Rahmen des Budgets 2023 einbringen.



Die FDS legt für das Jahr 2022 folgendes Prüfprogramm fest:

1. Zugriffsberechtigungen Geschäftsverwaltungssystem des Kantons (GEVER)
2. Arbeitsbesuch bei einer Gemeindefachstelle für Datenschutz

Zudem werden die Schengen-Kontrolle beim Migrationsamt fertig bearbeitet und die verschobene Prüfung der Lernfördersysteme durchgeführt.

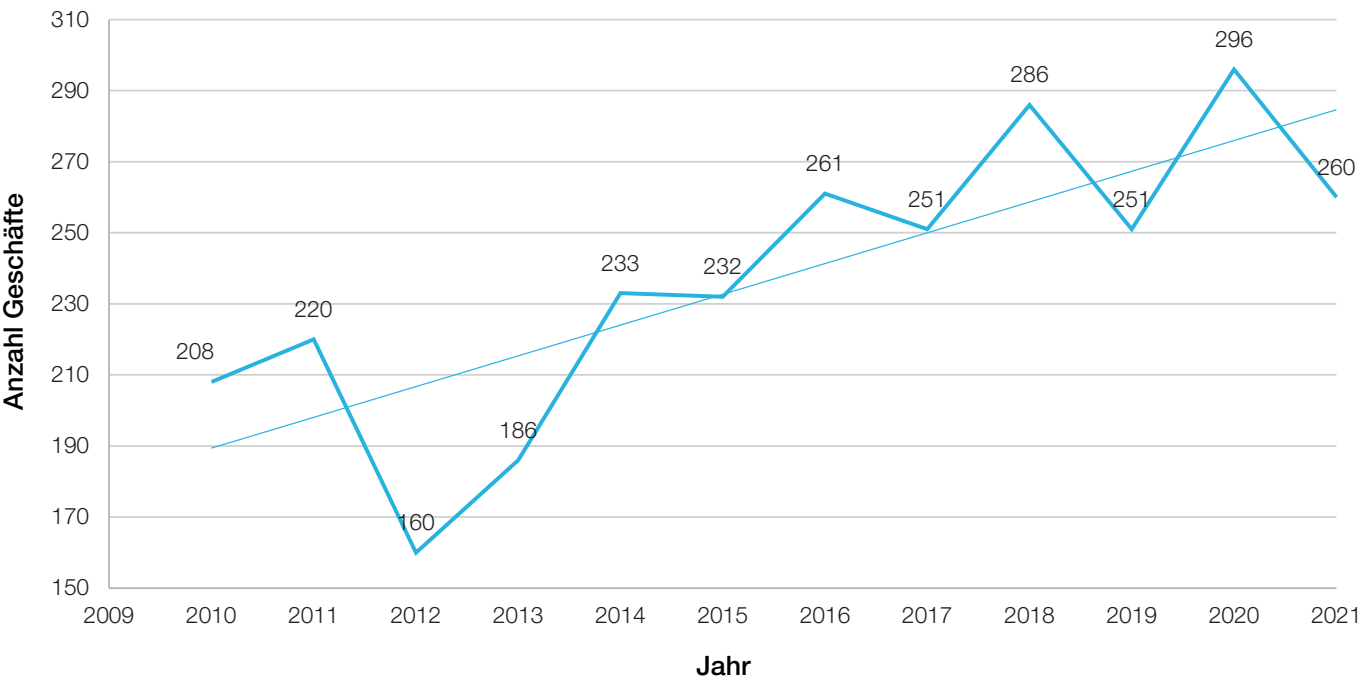
11 Antrag

Wir beantragen Ihnen, Frau Präsidentin, sehr geehrte Damen und Herren, auf den Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2021 einzutreten.

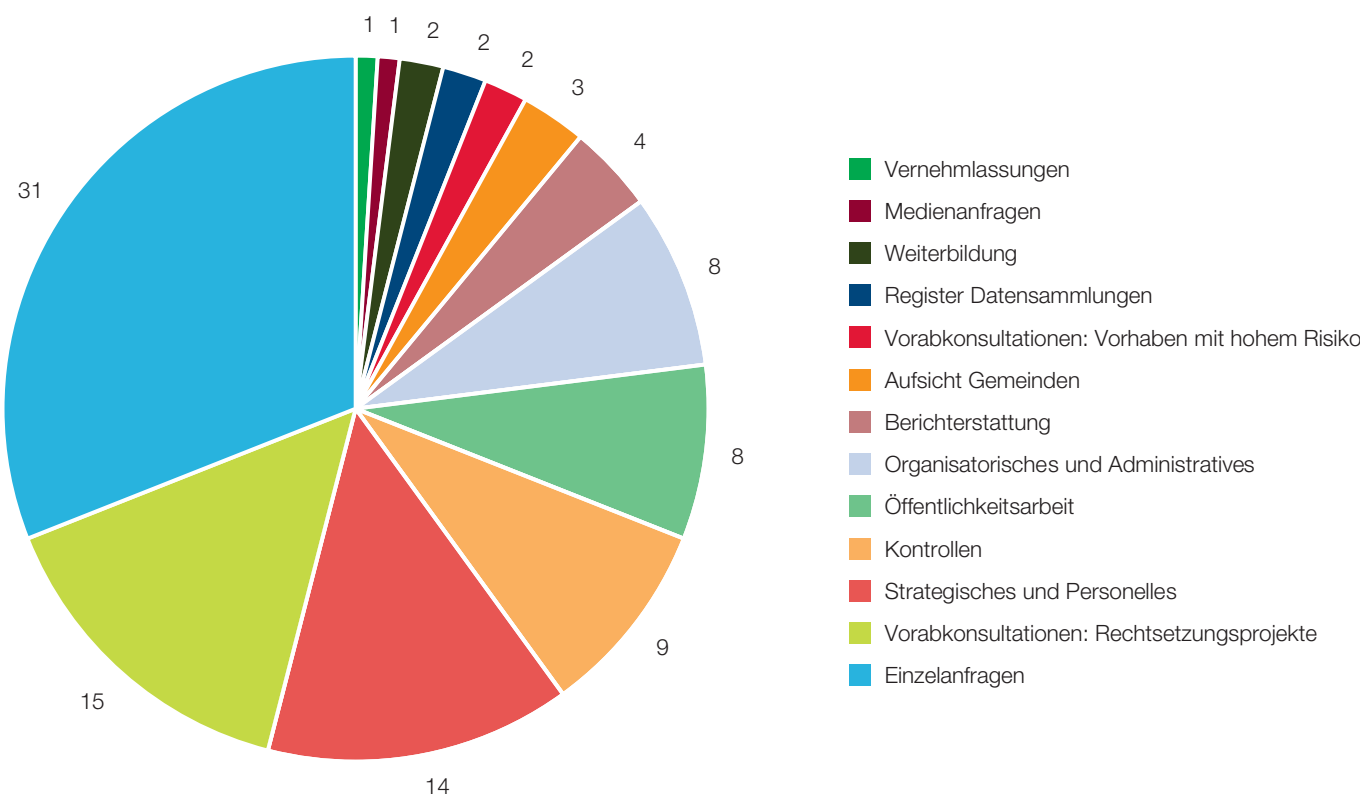
Kantonale Fachstelle für Datenschutz

Corinne Suter Hellstern, Leiterin

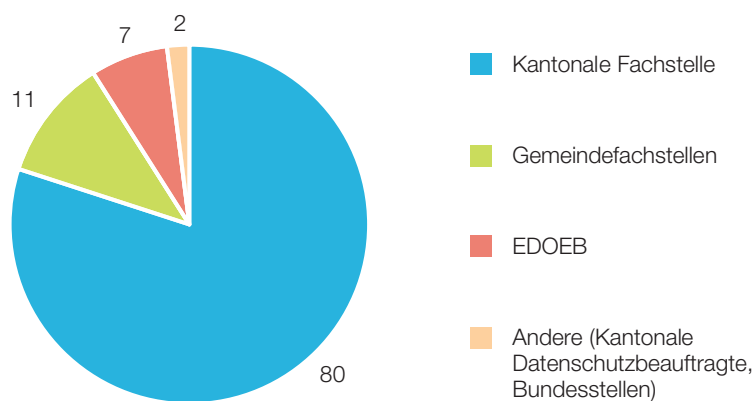
Geschäftseingänge



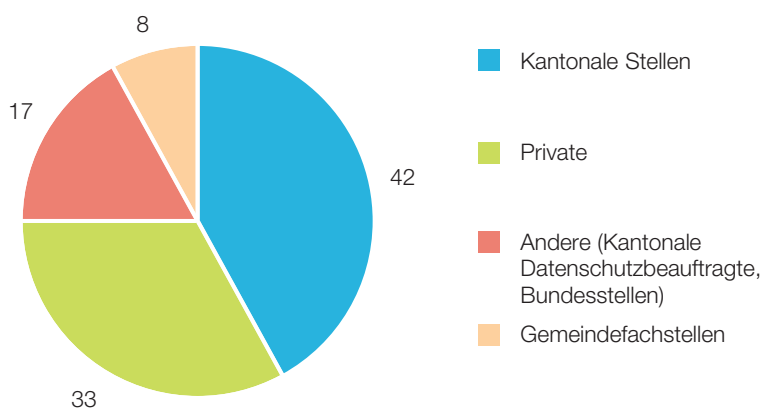
Aufgabenverteilung nach Art in Prozent



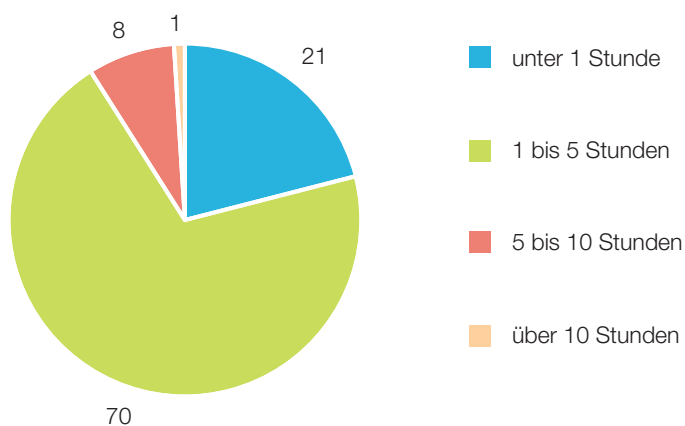
Zuständigkeit für Einzelanfragen in Prozent



Herkunft der Einzelanfragen in Prozent



zeitlicher Aufwand für Einzelanfragen in Prozent



Kantonsrat des Kantons St.Gallen

Geschäft 32.22.03

Fachstelle für Datenschutz

Regierungsgebäude, 9001 St.Gallen

Telefon: 058 229 14 14

E-Mail: datenschutz@sg.ch

Internet: www.datenschutz.sg.ch