Kanton St.Gallen
Fachstelle für Datenschutz

# Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2022

# Inhaltsverzeichnis

# 1 Zusammenfassung

*Die Geschäfte der Berichtsperiode verdeutlichen, dass die Komplexität der Aufgaben der Fachstelle für Datenschutz (nachfolgend FDS) weiter zunimmt. Zudem sind es nicht mehr zahlreiche Einzelfälle, welche die Ressourcen beanspruchen, sondern die sehr umfassenden Vorabkonsultationen, Kontrollen oder Datenschutzverletzungen. Sie gehören zu den zentralen Aufgaben der FDS. Damit einher geht, dass die Bearbeitung einzelner Geschäfte wesentlich länger dauert, indem sie etwa in Etappen beurteilt werden. So konnten im Berichtsjahr einige grosse Vorhaben noch nicht abgeschlossen werden. Gleichzeitig haben diese Geschäfte i.d.R. aber eine grössere Wirkung, beispielsweise bezüglich der Sensibilisierung, weil sie wichtige Themen und zahlreiche Personen betreffen.*

*Bisher verfügte die FDS über keine Ressourcen im Bereich IT. Mit der zunehmenden Digitalisierung wurde der Bedarf immer offensichtlicher. Auf das Jahr 2023 wurde der FDS eine IT-Audit-Stelle zugesprochen.*

*Seit dem Jahr 2019 müssen die kantonalen öffentlichen Organe Datenschutzverletzungen der FDS melden, wenn sie voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen. Einerseits dient dieses Instrument dem Schutz der betroffenen Personen. Anderseits dient es auch dazu, dass die öffentlichen Organe Datenschutz und IT-Sicherheit einen hohen Stellenwert beimessen, um einen allfälligen Reputationsschaden zu verhindern. Die Meldungen sollen auch eine Änderung der Unternehmenskultur bewirken hin zu einem offeneren Umgang mit solchen Vorfällen. Es geht nicht darum, das öffentliche Organ an den Pranger zu stellen, sondern darum, gute Lösungen zu finden, damit sich solche Vorfälle nicht wiederholen. Im Berichtsjahr bearbeitete die FDS zwei solche Meldungen.*

*Besonders aktuell ist derzeit Microsoft 365, also die Bearbeitung von Personendaten in der Cloud von Microsoft. Dabei stellen sich zahlreiche datenschutzrechtliche und technische Fragen. Ein öffentliches Organ, für das die rechtsstaatlichen Prinzipien gelten und das an die Grundrechte gebunden ist, muss sehr sorgfältig prüfen, ob und besonders welche Personendaten in einer solchen Cloud bearbeitet werden dürfen, und welche nicht.*

*Im Berichtsjahr machte die FDS eine Schengen-Kontrolle beim Migrationsamt. Es wurden keine Unregelmässigkeiten festgestellt. Die Bearbeitung durch die Mitarbeitenden machte einen guten und professionellen Eindruck. Die FDS gab Empfehlungen in den Bereichen Zugriffsberechtigung und Schulung ab. Bei der Prüfung der Zugriffe auf die kantonale Einwohnerdatenplattform machte die FDS Empfehlungen im Zusammenhang mit Zugriffen auf Datenfelder, die für die Aufgabenerfüllung nicht benötigt werden oder wofür die Rechtsgrundlage fehlte. Die beiden im Berichtsjahr durchgeführten Prüfungen des Lernfördersystems beim Lehrmittelverlag und des Geschäftsverwaltungssystems des Kantons sind noch nicht abgeschlossen.*

*Die FDS stattete der Datenschutzfachstelle Rapperswil-Jona einen Arbeitsbesuch ab. Sie erfüllt ihre Aufgaben gut, pflegt einen partnerschaftlichen Umgang mit den Gemeinden und achtet auf pragmatische Lösungen. Das dürfte es vielen Gemeinden erleichtern, von sich aus mit Fragen an die Fachstelle zu gelangen. Das ist wichtig, denn auch bei den Gemeinden ergeben sich zahlreiche Fragen mit zunehmender Komplexität. Inskünf-*

*tig dürfte sich auch für die Gemeindefachstellen für Datenschutz die Frage von IT-Know-how stellen. Eine Lösung könnte sein, dass die neu anzustellende Person bei der FDS punktuell auch für die Gemeindefachstellen tätig sein wird. Im Rahmen ihrer Aufsicht hat die FDS die Gemeindefachstellen für Datenschutz darauf hingewiesen, ein achtsames Auge auf das Thema Microsoft 365 bei den Gemeinden zu werfen. Solche Vorhaben sollen nicht ohne Beizug der Datenschutz-Fachstellen realisiert werden.*

*Im Berichtsjahr bearbeitete die FDS einige Vorhaben mit einem hohen Risiko für die Grundrechte betroffener Personen, so das Thema Videoüberwachung, die Bearbeitung in der Cloud von Microsoft oder die Datenbearbeitung in Pupil. Pupil ist eine Cloud-Softwarelösung im Bereich der Schulverwaltung. Dabei nutzen sämtliche Schulen die gleiche Software auf dem gleichen Server. Solche Lösungen, verbunden mit zahlreichen auch sensiblen Personendaten stellen sehr hohe Anforderungen an die Datensicherheit und an die korrekte und strenge Regelung der Zugriffsrechte. Besonders wichtig ist auch, dass Personen, die bei ihrem Schulträger für die Benutzer- und Berechtigungs-verwaltung verantwortlich sind, über eine adäquate Ausbildung verfügen. Wichtig ist zudem die Regelung der Verantwortlichkeiten. Zudem vertritt die FDS die Auffassung, dass genügende Rechtsgrundlagen geschaffen werden sollen.*

*Die FDS nahm zu verschiedenen Rechtsetzungs-Vorhaben Stellung, so auch zu jenen im Polizeigesetz. In der präventiven Polizeiarbeit sind verschiedene Neuerungen vorge-sehen: die Regelung des Datenaustausches, das Führen einer Gefährderliste oder das predictive policing. Die präventive Polizeiarbeit ist aus datenschutzrechtlicher Sicht sehr heikel, da ungesicherte Informationen ausserhalb eines formellen Verfahrens bearbeitet werden. An die Bestimmtheit der gesetzlichen Grundlagen müssen deshalb besonders hohe Anforderungen gestellt werden.*

*Im Rahmen von Einzelanfragen befasste sich die FDS u.a. mit den Themen von Video-konferenzen im Bereich der Arbeitslosenversicherung, der Anwendbarkeit des DSG auf die Pensionskasse und wir.impfen.ch.*

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 [2,3]. Der vorliegende Bericht gibt Rechenschaft über die Tätigkeit der FDS im Jahr 2022.

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, ABl 2008, 2299 ff., 2329.

# 2 Schwerpunkte

## 2.1 Meldepflicht Datenschutzverletzungen

Seit dem Jahr 2019 müssen die kantonalen öffentlichen Organe Datenschutzverletzungen der FDS melden, wenn sie voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen. Sinn der Meldepflicht ist einerseits, dass die von einer Datenschutzverletzung betroffenen Personen Massnahmen zu ihrem Schutz treffen können, wie z.B. die Sperrung von Zugängen oder die Änderung von Passwörtern. Anderseits sollen die öffentlichen Organe angehalten werden, Datenschutz und IT-Sicherheit einen hohen Stellenwert beizumessen. Sie sollen alle erforderlichen Massnahmen treffen, damit es nicht zu einer Datenschutzverletzung kommt. Damit können sie dadurch entstehende Aufwendungen und ein Reputationsverlust vermeiden. Die Meldungen sollen auch eine Änderung der Unternehmenskultur bewirken hin zu einem offeneren und transparenteren Umgang mit solchen Vorfällen. Es geht nicht darum, das öffentliche Organ an den Pranger zu stellen, sondern darum, gute Lösungen zu finden, damit sich solche Vorfälle nicht wiederholen. Aufgrund des geschilderten Sachverhalts gibt die FDS Empfehlungen ab und steht auch beratend zur Verfügung. Wichtig ist eine rasche Meldung, auch wenn noch nicht alle erforderlichen Angaben gemacht werden können. Haben die betroffenen Personen die Möglichkeit, einen allfälligen Schaden mit eigenen Vorkehren zu verkleinern, ist Zeit ein sehr wichtiger Faktor.

Die Meldepflicht spielte in den Vorjahren noch praktisch keine Rolle. Im Berichtsjahr wurden der FDS zwei Fälle gemeldet. Im einen Fall ging es um einen verlorenen unverschlüsselten USB-Stick mit sensiblen Daten. Die FDS empfahl zu prüfen, ob Daten abgeflossen waren, oder nicht. Zudem empfahl sie, die betroffenen Personen zu informieren, wenn ein Datenabfluss nicht ausgeschlossen werden konnte oder die Wahrscheinlichkeit dafür nicht sehr gering war. Es sollen nur noch verschlüsselte Sticks verwendet werden, sofern dieses Medium nach wie vor genutzt werden muss. Weiter sollte ein Prozess mit klaren Verantwortlichkeiten für die Meldung von Datenschutzverletzungen definiert werden. Gerade in Fällen, in denen von einer Datenschutzverletzung betroffene Personen selbst Vorkehren zum eigenen Schutz treffen können oder müssen ist es wichtig, dass sehr rasch gehandelt und informiert wird. Zudem sollte die Sensibilisierung optimiert werden. Der Vorfall soll sorgfältig dokumentiert und die Dokumentation aufbewahrt werden. Letzterer Punkt gilt für sämtliche Fälle von Datenschutzverletzungen, auch für diejenigen, bei denen keine Meldepflicht gilt. Es geht um die Beweispflicht, wozu das öffentliche Organ gemäss dem Datenschutzgesetz[4] verpflichtet ist.

Der zweite gemeldete Fall betraf die Bearbeitung von Personendaten in einem Bereich mit Zugangsbeschränkung. Während einer gewissen Zeit war es möglich, dass Personen Daten einsehen konnten, die sie für ihre Aufgabenerfüllung nicht benötigten. Nachdem das öffentliche Organ davon Kenntnis erlangte, sperrte es die Zugriffe unverzüglich. Dieser Fall ist noch nicht abgeschlossen, weil das öffentliche Organ noch Abklärungen tätigt, die es für die Auswertung braucht.

4 sGS 142.1.

## 2.2 Auftragsdatenbearbeitung

Die Datenschutzgesetzgebung lässt eine Bearbeitung von Personendaten durch Dritte unter bestimmten Voraussetzungen zu. In der Praxis ist diese Bestimmung sehr wichtig, immer mehr Daten werden im Auftrag bearbeitet. Dabei geht es vorwiegend um Bearbeitungen als Cloud-Lösung. Das ist eine Auftragsdatenbearbeitung mit erhöhtem Risiko. Insbesondere geht ein starker Kontrollverlust des öffentlichen Organs mit solchen Lösungen einher, ebenso eine hohe Abhängigkeit vom Auftragsdatenbearbeiter. Die erhöhten Risiken müssen mit geeigneten Massnahmen so weit gesenkt werden, dass sie tragbar werden. Nicht alle Arten von Personendaten dürfen in jeder beliebigen Cloud bearbeitet werden. In gewissen Konstellationen gibt es rechtliche Schranken, welche die Auslagerung nicht zulassen; so beispielsweise bei Personendaten, die einem Berufsgeheimnis oder besonderen Amtsgeheimnis unterliegen.

Besonders aktuell bei vielen Stellen ist derzeit Microsoft 365, also die Bearbeitung von Personendaten in der Cloud von Microsoft. Die Verträge der On-Premise Anwendungen, die derzeit im Einsatz sind, laufen aus und die On-Premise Anwendungen werden von Microsoft inskünftig teilweise nicht mehr unterstützt. Microsoft als US-Unternehmen untersteht dem dortigen Recht. Bekanntlich verfügen die USA nicht über ein vergleichbares Datenschutzniveau wie die Schweiz oder Länder der Europäischen Union (vgl. Staatenliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten). Dazu kommt der Cloud Act, der den US-Strafbehörden ohne Weg über die internationale Rechtshilfe ermöglicht, auf in- und ausländische Server Zugriff zu nehmen. Eine öffentliche Stelle, für welche die rechtsstaatlichen Prinzipien gelten und die an die Grundrechte gebunden ist, muss sehr sorgfältig prüfen, welche Personendaten in einer solchen Cloud bearbeitet werden dürfen, und welche nicht. Für die Bearbeitung derjenigen Personendaten, für welche die Bearbeitung in der Cloud rechtlich zulässig ist, müssen die entstehenden Risiken mit technischen und organisatorischen Massnahmen auf ein vertretbares Mass reduziert werden. Ist das nicht möglich, soll von dieser Datenbearbeitung abgesehen werden. Erforderlich ist eine sorgfältige Aufarbeitung aller Risiken mittels einer Datenschutz-Folgenabschätzung. Werden die Daten nicht verschlüsselt und liegt das Schlüsselmanagement nicht beim öffentlichen Organ, ist zudem eine Vorabkonsultation bei den Datenschutzfachstellen erforderlich.

Es gibt aber auch weitere Vorhaben im Bereich der Auftragsdatenbearbeitung: Eine Stelle liess Personendaten im Ausland scannen. Dabei handelt es sich ebenfalls um eine Auftragsdatenbearbeitung durch Dritte, es ist juristisch gesehen keine Datenbekanntgabe ins Ausland. Der Unterschied liegt unter anderem darin, dass bei der Auftragsdatenbearbeitung die Verantwortung beim öffentlichen Organ verbleibt. Also auch in diesem Fall bleibt das auslagernde öffentliche Organ dafür zuständig, dass die Personendaten konform mit dem DSG bearbeitet werden.

# 3 Prüftätigkeit

## 3.1 Migrationsamt (Schengen-Kontrolle)

Mit Anschluss der Schweiz an den Schengen-Raum haben einige kantonale Stellen (Polizei, Migrationsamt) Zugriff auf das Schengener Informationssystem erhalten. Dessen Handhabung muss durch die Kontrollinstanz regelmässig überprüft werden.[5] Die FDS ist Kontrollinstanz über die Bearbeitung von Personendaten durch öffentliche Organe des Kantons St.Gallen, die das nationale Schengener Informationssystem (N-SIS) benutzen.[6] Die FDS hat in ihrem Prüfprogramm 2020 eine Prüfung der Handhabung des N-SIS beim Migrationsamt vorgesehen. Wegen der Pandemie musste sie verschoben werden und wurde im Jahr 2022 durchgeführt. Gegenstand der Prüfung waren vorab Zugriffsberechtigung und Organisation sowie die Benutzung des Systems durch die Mitarbeitenden. Die FDS prüfte dies einerseits mit einer schriftlichen Befragung, anderseits führte sie eine Kontrolle der Logfiles ausgewählter Mitarbeitender durch.

Es wurden keine Unregelmässigkeiten festgestellt. Die Bearbeitung durch die Mitarbeitenden machte einen guten und professionellen Eindruck. Die FDS empfahl darauf zu achten, dass Zugriffsberechtigungen systematisch entzogen werden. Zudem ist die FDS der Ansicht, dass das Thema Datenschutz bei der Einführung neuer Mitarbeitender umfassender behandelt und danach regelmässig darauf sensibilisiert werden sollte.

5 Art. 55 der Verordnung über den nationalen Teil des Schengener Informationssystems und das SIRENE-Büro, SR 362.0.

6 Art. 114 f. Übereinkommen zur Durchführung des Übereinkommens von Schengen, Art. 55 der Verordnung über den nationalen Teil des Schengener Informationssystems und das SIRENE-Büro, SR 362.0.

## 3.2 Lernfördersysteme

Im Jahr 2022 prüfte die FDS die Lernfördersysteme des kantonalen Lehrmittelverlags. Themen waren vorab die Auftragsdatenbearbeitung, Löschung und Datenbekanntgabe, Schulung und Datensicherung sowie organisatorische Aspekte. Die Prüfung ist noch nicht abgeschlossen.

## 3.3 GEVER

Ende des Berichtsjahres prüfte die FDS Organisation und Zugriffsberechtigungen des elektronischen Geschäftsverwaltungssystems (GEVER) des Kantons. GEVER wird bis Ende 2023 schrittweise in der Zentralverwaltung, der Staatsanwaltschaft und bei den Gerichten eingeführt. Die Prüfung ist noch nicht abgeschlossen.

## 3.4 Zugriffe auf Kantonale Einwohnerdatenplattform

Die kantonale Einwohnerdatenplattform beinhaltet zahlreiche Personendaten 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 FDS hat bereits im Jahr 2021 Kontrollen gemacht und wird jährlich weitere Stellen prüfen. Geprüft wird einerseits, ob rechtliche Grundlagen vorhanden sind, welche die Bearbeitung dieser Personendaten rechtfertigen und andererseits, ob diese Personendaten für den Geschäftsprozess notwendig sind. Weiter wird die organisatorische Handhabung bei den Stellen geprüft.

Die im Jahr 2021 noch nicht abgeschlossenen Prüfungen [7] beim Amt für Soziales und drei Dienststellen des Gesundheitsdepartementes konnten abgeschlossen werden. Die FDS machte Empfehlungen im Zusammenhang mit Zugriffen auf Datenfelder, die für die Aufgabenerfüllung nicht benötigt werden. Bei einzelnen Dienststellen des Gesundheitsdepartementes waren diese teilweise deutlich zu umfangreich. Alle Stellen sicherten zu, den Umfang zu prüfen und zu reduzieren.

Im Berichtsjahr prüfte die FDS ausserdem die Zugriffe des Krebsregisters. Weil daran unter anderem auch die Kantone Appenzell Inner- und Ausserrhoden sowie Thurgau beteiligt sind, erfolgte die Prüfung in Abstimmung mit den Datenschutzbeauftragten dieser Kantone. Die FDS stellte fest, dass für die Abfrage zweier Datenfelder die Rechtsgrundlage fehlt und vereinzelt Personen auf Personendaten Zugriff haben, die sie für die gesetzliche Aufgabenerfüllung nicht benötigen. Sie empfahl, inskünftig auf diese Zugriffe zu verzichten. Zusätzlich zum Zugriff auf KEWR erhält das Krebsregister von den Einwohnerämtern Excel-Listen mit Personendaten aller Bürgerinnen und Bürgern. Auf diese Weise kann zwar ein Rückschluss der Gemeinde auf eine Krebserkrankung einer bestimmten Bürgerin bzw. eines bestimmten Bürgers vermieden werden. Dieses Vorgehen widerspricht allerdings dem Verhältnismässigkeitsprinzip und dem Grundsatz der Datensparsamkeit, weil das Krebsregister Personendaten erhält, die es nicht benötigt. Die FDS empfahl deshalb, dafür eine datenschutzkonforme Lösung zu suchen.

7 Siehe dazu Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2021, S. 9.

# 4 Aufsicht und Beratung Gemeindefachstellen

## 4.1 Arbeitsbesuch

Im Berichtsjahr stattete die FDS zusammen mit dem Dienst für Informatikplanung (DIP) der Fachstelle für Datenschutz Rapperswil-Jona (nachfolgend FS) einen Arbeitsbesuch ab. Bei Organisation und Zuständigkeiten hat sich gegenüber früheren Besuchen nichts geändert. Die FS berichtete über die Tendenz, dass die Fallzahlen stagnieren, die Komplexität der einzelnen Geschäfte aber stark zunimmt. Ein Anliegen der FS ist, dass sie für zusätzliche Gemeinden die Funktion der Datenschutz-Fachstelle übernehmen könnte, das Einzugsgebiet heute ist eher klein. Damit könnte verstärkt Know-how aufgebaut und in Weiterbildung investiert werden. Diesbezüglich war sie mit anderen Datenschutz-Fachstellen in Kontakt, bisher hat sich aber keine Lösung ergeben.
Die FS erfüllt ihre Aufgaben gut. Sie pflegt einen partnerschaftlichen Umgang mit den Gemeinden und achtet auf pragmatische Lösungen. Das dürfte es vielen Gemeinden erleichtern, von sich aus mit Fragen an die FS zu gelangen. Das ist wichtig, ergeben sich doch auch bei den Gemeinden zahlreiche datenschutzrechtliche Fragen mit zunehmender Komplexität. Als sehr wichtig erachtet die FDS die stete Information und Sensibilisierung bezüglich der Instrumente der Datenschutz-Folgenabschätzung, der Vorabkonsultation und der Meldepflicht bei Datenschutzverletzungen. Die FS bearbeitete bisher weder Vorabkonsultationen noch Meldepflichten. Es ist kaum anzunehmen, dass bei den Gemeinden keine solche Geschäfte anfallen. Nur schon die Diskussion um Microsoft 365 bei den Gemeinden zeigt, dass es sehr wohl Geschäfte gibt, die einer Datenschutz-Folgenabschätzung bedürfen oder der FS zur Vorabkonsultation vorgelegt werden müssen.

Bisher benötigte die FS keine Ressourcen im Bereich IT. Mit der zunehmenden Digitalisierung ändert sich dies. Auf das Jahr 2023 wurde der FDS eine IT-Audit-Stelle zugesprochen. Es wäre sinnvoll, wenn diese Person punktuell ihr Know-how auch den Gemeindefachstellen zur Verfügung stellt, sofern nötig und gewünscht. Die FS zeigte sich am Angebot interessiert. Zudem hat die FDS angeregt, den Hinweis auf der eigenen Homepage auf die Funktion als Datenschutzbehörde besser ersichtlich zu machen und gleichzeitig auf Arbeitshilfen für die Gemeinden zu verweisen.

## 4.2 Microsoft 365

Im Rahmen ihrer Aufsichtstätigkeit hat die FDS die Gemeindefachstellen für Datenschutz darüber informiert, dass Vorhaben rund um Microsoft 365 sehr aufmerksam verfolgt werden sollen. Es handelt sich dabei um sehr komplexe datenschutzrechtliche Fragen, die geklärt werden müssen. Zudem ist eine Vorabkonsultation (und vorgängige Datenschutz-Folgenabschätzung durch die Gemeinden) erforderlich.

## 4.3 Zusammenarbeit Gemeindefachstellen

Die Datenschutz-Fachstelle der Stadt St.Gallen und die FDS pflegen mit eGovernment St.Gallen digital einen regelmässigen Erfahrungsaustausch. Dabei nimmt die Datenschutz-Fachstelle der Stadt auch die Interessen der anderen Gemeindefachstellen für Datenschutz wahr. Die FDS begrüsst dies sehr und regt an, die Zusammenarbeit unter den Gemeindefachstellen für Datenschutz auch in weiteren Bereichen zu pflegen. Es stellen sich häufig dieselben Fragen und das Rad muss nicht immer neu erfunden werden.

## 4.4 Erfahrungsaustausch

Am Erfahrungsaustausch der FDS mit den Gemeindefachstellen für Datenschutz waren die kantonale Einwohnerdatenplattform und das Personenregister Thema. Zudem wie bereits beim Arbeitsbesuch die Instrumente der Datenschutz-Folgenabschätzung und Vorabkonsultation und allgemein die Datenschutz-Schulung der Gemeinden.

# 5 Vorhaben mit hohem Risiko

## 5.1 Zeitrafferfilm Square

Im Jahr 2020 nahm die FDS Stellung zur Webcam beim Square (ehemals Learning Center) der Universität St.Gallen. Die Verantwortlichen des Square beabsichtigten, von den Bildern der Webcam einen Zeitraffer-Film zu veröffentlichen. Die FDS machte damals u.a. die Empfehlung, dass dieser vor der Veröffentlichung der FDS vorgelegt werden muss. Das haben die Verantwortlichen des Square im Berichtsjahr getan. Weil teils Personen noch bestimmbar waren empfahl die FDS, den im Video gezeigten Filmausschnitt zu verkleinern und im Bereich Trottoir / Strasse einen stärkeren Filter zu verwenden. Dies wurde so umgesetzt.

## 5.2 Videoüberwachung Spital

Ein Spital beabsichtigt, Videoüberwachung in verschiedenen Bereichen einzusetzen. Bezweckt werden soll damit die sichere medizinische Versorgung, die Sicherheit der Mitarbeitenden, Patientinnen und Patienten sowie der Besuchenden und die Durchführung von Weiterbildung. Aufgrund der eingereichten Unterlagen machte die FDS eine erste Vorabkonsultation. Bekanntlich gibt es bisher keine formell-gesetzliche Grundlage für Videoüberwachung im Kanton. Videoüberwachung ist also, falls überhaupt, bei kantonalen Stellen nur in einem sehr eng begrenzten Rahmen zulässig. Für eine Videoüberwachung ist aber nicht nur eine Rechtsgrundlage erforderlich, sondern sie muss auch verhältnismässig sein. Die Verhältnismässigkeit der einzelnen Kameras kann nicht aufgrund von Unterlagen beurteilt werden. Deshalb nahm die FDS einen Augenschein vor Ort vor. Die Abklärung, ob und wenn ja welche Videoüberwachung zulässig ist, läuft derzeit noch.

Bei einer weiteren Stelle war die FDS vor Ort: Dort wird eine Echtzeitbeobachtung eingesetzt. Bisher fehlt eine Datenschutz-Folgenabschätzung, welche die Stelle derzeit erarbeitet und anschliessend der FDS zur Vorabkonsultation einreicht.

## 5.3 PUPIL

Pupil ist eine aus verschiedenen Modulen bestehende umfassende Cloud-Softwarelösung im Bereich der Schulverwaltung und soll u.a. «LehrerOffice» ablösen. Alle Volksschulen im Kanton müssen ab dem Jahr 2025 PUPIL nutzen. Die Daten von Schülerinnen und Schülern werden vollständig digital gehalten, sei es im Bereich der Schullaufbahn, der Tagesschulstrukturen oder der Organisation des Schulbusses. Bei einem Schulübertritt ist sichergestellt, dass die Daten in einem kompatiblen Format verfügbar sind. Die eingesetzte Software ist mandantenfähig, das bedeutet, eine Schule kann nur ihre Daten einsehen, obwohl sämtliche Schulen die gleiche Software auf dem gleichen Server nutzen. In der Schulsoftware werden die Daten von Schülerinnen und Schülern während der gesamten Schullaufbahn in der Volksschule bearbeitet. Neben der grossen Zeitspanne kommt hinzu, dass Daten in sehr vielen Bereichen bearbeitet werden, darunter auch besonders schützenswerte Personendaten, etwa Arztbesuche oder sonderpädagogische Massnahmen. Die sehr hohe Dichte an Personendaten verbunden mit einer Softwarelösung, die technisch einfache Zugangsmöglichkeiten bietet, stellt sehr hohe Anforderungen an die Datensicherheit und an die korrekte und strenge Regelung der Zugriffsrechte. Im Folgenden ist die Berichterstattung darüber etwas ausführlicher, da inskünftig damit zu rechnen ist, dass vermehrt solche Anwendungen eingesetzt werden.

Die FDS wurde eingeladen zur Frage Stellung zu nehmen, ob Pupil eine explizite Rechtsgrundlage benötige: Derzeit kennt das Volksschulgesetz keine Bestimmung zur Bearbeitung von Personendaten. Die Digitalisierung führt dazu, dass das Grundrecht auf Privatsphäre viel stärker gefährdet ist, als in der analogen Welt. Somit erhält der Schutz der Personendaten auch einen anderen Stellenwert. Einerseits sind unrechtmässige Datenbearbeitungen einfacher und v.a. in viel grösserem Umfang möglich. Anderseits geht die Transparenz der Datenbearbeitungen für die betroffenen Personen zunehmend verloren angesichts der zahlreichen Involvierten und den entsprechenden Datenflüssen. Gemäss einem Entscheid des Bundesgerichts muss für die betroffenen Personen aber nachvollziehbar sein, was die Konsequenzen ihres Verhaltens sind.[8] All dies erfordert eine erhöhte Anforderung an die rechtlichen Bestimmungen. Diese müssen so präzis und transparent sein, dass die Betroffenen die Konsequenzen erkennen können. Eine genügende formell-gesetzliche Regelung erfordert deshalb explizite, hinreichend bestimmte Regelungen. Die FDS empfiehlt, solche zu schaffen.

8 Die Rechtsgrundlage muss gemäss Bundesgericht so präzis sein, dass Bürgerinnen und Bürger ihr Verhalten danach richten und die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit erkennen können, BGE 117 Ia 472 E. 3e.

Nebst der Rechtsgrundlage äusserte sich die FDS allgemein zum Projekt: Die Projektleitung von pupil macht einen guten Eindruck. In anderen Bereichen machte die FDS verschiedene Empfehlungen: Die Festlegung, welche Benutzerrolle auf welche Datenfelder Lese- oder Schreibrechte hat, ist einer der für den Datenschutz essentiellen Punkte in einem Vorhaben wie Pupil. Personen dürfen nur Zugriffsrechte haben, wenn sie die Daten für die gesetzliche Aufgabenerfüllung benötigen. Auch die Dauer der Zugriffsrechte muss geprüft werden, da allenfalls nicht sämtliche zugriffsberechtigte Personen über den ganzen Zeitraum der Aufbewahrung Zugriff haben müssen. Die Zugriffsrechte müssen zudem regelmässig überprüft werden. Ein besonderes Augenmerk muss auch den Superusern – Personen, die für die Benutzer- und Berechtigungsverwaltung bei ihrem Schulträger verantwortlich sind – gelten. Sie haben direkten Einfluss auf die Einsichtsmöglichkeiten einer Person. Ihrer Verantwortung entsprechend sollten sie über eine adäquate Ausbildung verfügen.

Bei Pupil handelt es sich um eine Auftragsdatenbearbeitung, Gerichtsstand und Serverstandort sind in der Schweiz. Zu beachten ist die Thematik der Unterauftragsnehmer: Für diese gelten dieselben Anforderungen, wie für den Auftragsdatenbearbeiter selbst und das öffentliche Organ muss der Übertragung an einen Subunternehmer vorgängig schriftlich zustimmen.

Wichtig ist auch das Prinzip, dass richtige Daten bearbeitet werden. Gerade bei den schulischen Leistungen und der Gesundheit besteht ein sehr grosser Einfluss auf die Schul- und spätere berufliche Laufbahn von Schülerinnen und Schülern. So muss etwa sichergestellt werden, dass nur wenige Personen Schreibrechte haben. Wichtig ist, ein Löschkonzept zu erstellen. Personendaten, deren Aufbewahrungsdauer abgelaufen ist müssen vorbehältlich der Ablieferung ans Staatsarchiv automatisch gelöscht werden.

Bei der Implementierung von Pupil sind mehrere öffentliche Organe involviert: Unter anderem das Bildungsdepartement, das Amt für Volksschule, die Projektleitung innerhalb dieses Amts, eGovernment St.Gallen digital, die politischen Gemeinden sowie die Schulträger der Gemeinden. Bei einer solchen Vielzahl von Akteuren ist es unerlässlich, dass die Verantwortlichkeiten auch im Bereich Datenschutz klar geregelt sind. Dies spielt etwa bei der Meldung einer Datenschutzverletzung eine Rolle, bei der, wie oben dargelegt, teilweise sehr rasch gehandelt werden muss. Deshalb muss vorgängig ein klarer Prozess definiert werden. Die klare Regelung der Verantwortlichkeit ist auch für die Betroffenenrechte wichtig.

Pupil nutzt für die Kommunikation mit den Erziehungsberechtigten eine App (Messenger) für Smartphones. Die App war nicht Gegenstand der Vorabkonsultation und wird im Jahr 2023 geprüft.

## 5.4 Microsoft 365 bei Spital

Ein Spital beabsichtigte, seine bei Microsoft bisher On-Premise bezogenen IT-Dienstleistungen in die Cloud von Microsoft zu verlagern. Wie oben ausgeführt, gelten die USA nicht als Land mit einem angemessenen Datenschutzniveau. Mit dem Cloud Act behält sich der amerikanische Staat zudem vor, jederzeit auf die von Microsoft bearbeiteten Daten Zugriff nehmen zu können. Dem Cloud-Act unterstehende Anbieter müssen US-Behörden auch dann Zugriff auf gespeicherte Daten gewähren, wenn die Speicherung nicht in den USA, sondern in einem EU-Mitgliedstaat oder in der Schweiz erfolgt. Nicht alle Daten dürfen in einer solchen Cloud bearbeitet werden. Für die Auslagerung ist deshalb eine Klassifizierung der Daten zwingend um beurteilen zu können, welche Daten ausgelagert werden dürfen, und welche nicht. Die FDS machte zudem u.a. folgende Empfehlungen: Microsoft darf die Daten nur für Zwecke der Auftragserfüllung zugunsten des Spitals nutzen. Die Nutzung zu eigenen Zwecken ist nicht zulässig. Das muss vertraglich geregelt werden. Es muss zudem geregelt werden, was im Fall einer Kündigung des Vertrags geschieht. Es muss regelmässig geprüft werden, welche alternativen Lösungen bestehen. Die oben unter Ziff. 2.2 aufgeführten Voraussetzungen gelten zudem generell für alle Stellen, welche die Bearbeitung in der Cloud von Microsoft prüfen.

## 5.5 Workplace 2024

Im Berichtsjahr nahm die FDS Stellung zum Workplace 2024 (WP 2024). Dabei geht es darum, den heutigen digitalen Arbeitsplatz, der seit 2015 in Betrieb ist, abzulösen. Das Vorhaben betrifft Themen wie Identitäten, Berechtigungen oder Anbindung an die Cloud. Dabei stellen sich verschiedene Fragen, die teilweise auch mit der Frage der Datenbearbeitung in der Microsoft Cloud überlappen. Die FDS ist der Ansicht, dass sorgfältig geprüft werden muss, ob die heutigen Rechtsgrundlagen genügen. Zwar handelt es sich um eine Hilfsaufgabe, wofür i.d.R. keine speziellen zusätzlichen Rechtsgrundlagen nötig sind. Allerdings ist die papierene oder auch die digitale Datenbearbeitung on premise nicht zu vergleichen mit jener in einer Cloud eines internationalen Unternehmens. Es stellt sich die Frage, ob die Rechtsgrundlagen noch genügend bestimmt sind, damit Bürgerinnen und Bürger mögliche Konsequenzen abschätzen können. Des Weiteren muss die Verhältnismässigkeit für den Einsatz jedes einzelnen Dienstes geklärt werden. Subunternehmer aus einem Land mit einem nicht angemessenen Datenschutzniveau gemäss Staatenliste (siehe oben Ziff. 2.2) müssen bei einer Weiterübertragung ausgeschlossen werden. Wichtig ist, die Daten zu klassifizieren. Personendaten, die einem Geheimnis unterstehen (Berufsgeheimnis, besonderes Amtsgeheimnis) dürfen nicht in eine Cloud eines Unternehmens ausgelagert werden, das in einem Land ohne angemessenes Datenschutzniveau ansässig ist und rechtlich verpflichtet werden kann – ohne Weg über die internationale Rechtshilfe – staatlichen Stellen Personendaten bekanntzugeben. Ein weiterer wichtiger Punkt ist, dass das öffentliche Organ das Kontrollrecht vertraglich regelt. Ein solches Vorhaben birgt die Gefahr eines Kontrollverlusts und von Abhängigkeiten. So stellt sich auch die Frage was geschieht, wenn der Vertrag z.B. wegen einer Vertragsverletzung gekündigt werden muss.

# 6 Rechtsetzung

## 6.1 Nachträge zum Polizeigesetz

In der präventiven Polizeiarbeit sind verschiedene Neuerungen vorgesehen, so etwa das predictive policing, die Führung einer Gefährderliste oder Regelungen zum Datenaustausch. Die präventive Polizeiarbeit ist in datenschutzrechtlicher Hinsicht sehr heikel: Es werden Personendaten nicht im Rahmen eines formellen Verfahrens bearbeitet, sondern ungesicherte Informationen verwendet. Es muss vermieden werden, dass umfangreiche Datensammlungen nur aufgrund eines vagen Verdachts entstehen. Die Fichenaffäre in den 80er Jahren hat gezeigt, wohin solche Entwicklungen führen. Allerdings mit dem Unterschied, dass damals Papierakten geführt wurden, während dem heute alles elektronisch bearbeitet wird, was ein erheblich höheres Risiko für das Grundrecht auf Privatsphäre darstellt. An die gesetzlichen Grundlagen müssen daher besonders hohe Anforderungen gestellt werden.

Vorgesehen ist, das «predictive Policing» zu regeln. Es ist wichtig, dass diskutiert wird, ob der Einsatz dieses Instrumentes politisch und gesellschaftlich erwünscht ist. Der Einsatz ist unter anderem nur rechtmässig, wenn die Resultate zuverlässig sind, ansonsten die Verhältnis- und damit die Rechtmässigkeit nicht gegeben sind. Mit der «Gefährderliste» ist es möglich, dass Personen, die sich kein strafrechtlich justiziables Verhalten zuschulden haben kommen lassen, ohne durch ein Gericht angehört, in dieser Liste aufgeführt werden. Damit besteht die Gefahr einer Vorverurteilung. Das ist für den Persönlichkeitsschutz sehr heikel. Die Aufbewahrungsdauer muss definiert werden, ansonsten die Gefahr der ewigen Aufbewahrung besteht. Somit würde jemand als «ewiger Gefährder» gelten, was nicht verhältnismässig ist. Zudem stellt sich die Frage, ob die betroffenen Personen nicht wenigstens nachträglich darüber informiert werden müssen, dass ihre Daten in der Gefährderliste bearbeitet wurden.

Die vorgesehene Meldepflicht verschiedener Berufsgruppen birgt die Gefahr der Aushöhlung des Berufsgeheimnisses. Gerade im medizinischen Bereich ist es für den Aufbau eines Vertrauensverhältnisses sehr wichtig, dass es ein intaktes Berufsgeheimnis gibt. Allgemein waren nach Ansicht der FDS die Umschreibung der bearbeiteten Personendaten und der Zweck der Datenbearbeitung zu wenig präzis.

Bei der Regelung zum polizeilichen Datenaustausch fehlen präzise und abschliessende Bestimmungen. Verschiedene Aspekte wie Speicherdauer und Datenvernichtung müssen im Gesetz selbst geregelt werden. Zudem muss stets klar sein, wer die Datenhoheit hat und bei wem die Verantwortlichkeit liegt.

## 6.2 Nachtrag zum Steuergesetz

Es soll eine Meldepflicht für Arbeitslosenkassen eingeführt werden. Neu sollen nicht mehr die als arbeitslos gemeldeten Personen ihre Lohnausweise dem Steueramt senden, sondern die Arbeitslosenkasse soll verpflichtet werden, die jährlichen Lohnabrechnungen direkt zu übermitteln, wobei dies elektronisch erfolgen soll. Das Arbeitslosenversicherungsgesetz sieht vor, dass Stellen, welche mit der Durchführung des Gesetzes betraut sind, den kantonalen Steuerbehörden die Leistungsabrechnung direkt übermitteln können, sofern das kantonale Recht diese Möglichkeit vorsieht und sofern kein überwiegendes Privatinteresse entgegensteht. Diese Übermittlung soll über das einheitliche Lohnmeldeverfahren erfolgen, dessen technische Umsetzung aktuell vorbereitet wird.

Die FDS qualifizierte die Personendaten, welche bekannt gegeben werden sollen, als besonders schützenswert, womit erhöhte Anforderungen gelten. Das allgemeine Argument, eine Datenbearbeitung vereinfache den Geschäftsprozess, vermag allein keinen Grundrechtseingriff zu rechtfertigen. Nebst der Rechtsgrundlage muss die Verhältnismässigkeit beurteilt werden. Einerseits handelt es sich dabei um einen Grundsatz mit Verfassungsrang. Anderseits ergibt er sich direkt aus dem Arbeitslosenversicherungsgesetz, wonach keine überwiegenden Privatinteressen der Bekanntgabe entgegenstehen dürfen. Bei einer systematischen Datenbekanntgabe kann nicht beurteilt werden, ob überwiegende Privatinteressen der Bekanntgabe entgegenstehen. Damit widerspricht die Bestimmung dem Verhältnismässigkeitsgrundsatz.

## 6.3 Weitere

Die FDS nahm zudem zu folgenden weiteren Erlassen Stellung:

- V. Nachtrag zur Mittelschulverordnung
- XIII. Nachtrag zum Einführungsgesetz zur Bundesgesetzgebung über die Krankenversicherung
- Datenaustauschvereinbarungen Dienst für politische Rechte und Krebsregister

## 6.4 Ausserkantonale Erlasse

Die FDS nahm zu folgenden ausserkantonalen Erlassen und Vorhaben Stellung:

- Bundesgesetz über den Nachrichtendienst
- Flugpassagierdatengesetz
- Mehrwertsteuergesetz und Mehrwertsteuerverordnung
- Bundesgesetz über die Informationssicherheit beim Bund
- Abkommen zwischen der Schweiz und dem Fürstentum Liechtenstein über den Austausch von Daten betreffend gesperrte Spielerinnen und Spieler im Geldspielbereich
- Fragebogen der Europäischen Kommission zur Schengen-Evaluierung 2023

# 7 Einzelanfragen

## 7.1 Allgemeines

Wie in jedem Jahr bearbeitete die FDS zahlreiche Einzelanfragen. Die Themen waren breit gestreut, von Datenbekanntgaben an verschiedene Stellen über die Aufbewahrungspflicht bis zur Adressbekanntgabe für Vorsorgeprogramme. Auch Fragen zu dem im Jahr 2019 eingeführten Instrument der Datenschutz-Folgenabschätzung wurden der FDS gestellt, allerdings nicht mehr so zahlreich wie in den Vorjahren. Das deutet darauf hin, dass dieses wichtige Instrument bei kantonalen Stellen mehr oder weniger bekannt ist.

## 7.2 Videokonferenzen

Die regionalen Arbeitsvermittlungszentren setzen neben Vor-Ort- und Telefongesprächen auf Videogespräche mit der Applikation Zoom for Business. Stellensuchende bewegen sich beim Kontakt mit dem RAV in einem sensiblen Bereich. Der Einsatz von online übertragenen Videogesprächen kann bei ihnen, aber auch bei den Mitarbeitenden, Zweifel auslösen hinsichtlich der Datensicherheit; Sowohl bei der Übertragung des Gesprächs, als auch bei der Speicherung von allfälligen Daten.

Die FDS ist der Ansicht, dass ein Einsatz von Zoom weder für die Mitarbeitenden noch für die Stellensuchenden verpflichtend sein darf: Der Einsatz von Zoom ist in «gewöhnlichen» Zeiten nicht erforderlich für die gesetzliche Aufgabenerfüllung. Somit ist die Verhältnismässigkeit nicht gegeben. Es ist deshalb zwingend, dass ohne negative Konsequenzen für Stellensuchende und Mitarbeitende eine andere, datenschutzrechtlich unbedenkliche Möglichkeit wie ein Vor-Ort-Gespräch angeboten werden muss.

## 7.3 Anwendbarkeit DSG Pensionskasse

Zur Diskussion stand die Anwendbarkeit des DSG auf die St.Galler Pensionskasse (nachfolgend sgpk). Die sgpk ist eine öffentlich-rechtliche Stiftung mit Sitz in St.Gallen und vollzieht regelmässig Bundesrecht. Sie ist nicht Teil der zentralen Staatsverwaltung, sondern rechtlich, organisatorisch und finanziell verselbständigt und aus der Verwaltungsstruktur herausgelöst. Sie nimmt ihre Aufgabe als sachlich dezentralisierte Verwaltungseinheit wahr. Obwohl das DSG die öffentlich-rechtlichen Stiftungen nicht explizit erwähnt, ist die FDS der Auffassung, dass die sgpk ein kantonales öffentliches Organ ist.

Die sgpk ist aber nicht nur für den Kanton tätig, sondern u.a. auch für Träger der öffentlichen Volksschule. In diesen Fällen ist zwar das DSG anwendbar, die Aufsicht liegt aber bei den Gemeindefachstellen für Datenschutz. Sofern die sgpk Aufgaben für weitere Arbeitgeberinnen bzw. Arbeitgeber erfüllt, liegt die Zuständigkeit i.d.R. beim eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten.

## 7.4 wir.impfen.ch

Im Zusammenhang mit der Homepage wir-impfen.ch haben sich verschiedene Bürgerinnen und Bürger an die FDS gewendet.[9] Gegenstand der Fragen war hauptsächlich die Handhabung bzw. Architektur der Homepage, also Fragen technischer Natur. Die FDS konnte einige Fragen selber klären, für die Klärung der übrigen Fragen beauftragte sie eine externe IT-Fachperson mit der Analyse. Die Fragen der Bürgerinnen und Bürger konnten beantwortet werden.

Aufgrund der Prüfung stellte die FDS fest, dass Fragen offen waren: Einerseits wurde keine Datenschutz-Folgenabschätzung der Datenbearbeitung gemacht, um die Risiken einschätzen und mittels Massnahmen gegebenenfalls reduzieren zu können. Zudem waren die Fragen der Aufbewahrungsfrist und Löschung bzw. Vernichtung der Personendaten nicht geklärt. Im Vertrag mit dem Auftragsdatenbearbeiter fehlten Bestimmungen, so zu den Modalitäten im Fall eines Beizugs von Unterauftragsnehmern. Schliesslich fehlten Dokumente vorab im technischen Bereich wie Berechtigungsmodell oder Datenflussdiagramm. Aufgrund der Empfehlung der FDS klärte das öffentliche Organ die Fragen, reichte die Unterlagen im Wesentlichen nach und ergänzte den Vertrag mit dem Auftragsdatenbearbeiter. Noch in Diskussion sind die Fragen der Aufbewahrungsfristen und Löschung bzw. Vernichtung.

9 Siehe dazu Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2021, S. 16.

## 7.5 Zugriffsrechte Bewerbertool

Die Fachstelle für Datenschutz klärte ab, über welche Zugriffsrechte das Personalamt beim Bewerbertool des Kantons verfügt und inwieweit diese den datenschutzrechtlichen Vorgaben entsprechen.

Das Personalamt verfügt über weitgehende, ständige Zugriffsrechte für den fachlichen und technischen Support sowie für die Beratung von Personaldiensten. Die Zugriffsrechte dürfen nur bei einer konkreten Anfrage genutzt werden und werden protokolliert. Für den fachlichen und technischen Support erachtet die FDS die ständigen Zugriffsrechte als rechtmässig. Es verhindert einen unverhältnismässigen administrativen Aufwand, der entstehen würde, wenn bei jeder Anfrage Zugriffsrechte beantragt bzw. erteilt werden müssten.

Bei der Beratung ist die FDS jedoch anderer Ansicht: Die Stellensuchenden haben kein Arbeitsverhältnis mit dem Kanton. Bei einem grossen Teil dieser Personen erfolgt ein negativer Bescheid bereits nach der Prüfung des Dossiers durch die vorgesetzte Person (allenfalls noch in Absprache mit dem Personaldienst). Das Personalamt wird in dieser Phase sehr selten beigezogen. Ein ständiges Zugriffsrecht auf die sensiblen Daten einer grossen Anzahl Personen, die nicht in einem Arbeitsverhältnis zum Kanton stehen, ist aus Sicht der FDS unverhältnismässig, selbst wenn der Zugriff erst auf Anfrage genutzt werden darf. Die Zugriffsrechte bei Bedarf einzurichten, bedeutet in diesem Bereich aufgrund der Seltenheit keinen unverhältnismässigen Aufwand. Das Personalamt hat die Zugriffsrechte entsprechend angepasst.

# 8 Register und Verzeichnis der Bearbeitungstätigkeit


Zum Register der Datensammlungen wurden ein paar wenige Anfragen bearbeitet, etwa ob das Register immer noch geführt werden müsse und ob Lieferanten-Verträge ebenfalls aufgeführt werden müssen. Zum Verzeichnis der Bearbeitungstätigkeit stellten sich im Berichtsjahr keine Fragen.

# 9 Zusammenarbeit und Sensibilisierung

Wie in den vergangenen Jahren pflegte die FDS Austausch mit verschiedenen Stellen beim Kanton, die beim Datenschutz eine wichtige Rolle spielen.

Die Zusammenarbeit mit privatim, der Vereinigung der Schweizerischen Datenschutzbeauftragten, findet hauptsächlich im Rahmen der Vorstandsarbeit und an den zwei Mal jährlich stattfindenden Plenen statt. Die Datenschutzbeauftragten der Ostschweizer Kantone pflegen zudem eine regelmässige Zusammenarbeit mit Austausch über aktuelle Themen.

Wie jedes Jahr erarbeitete die FDS eine Sequenz für das e-Learning Datenschutz und IT-Sicherheit des Kantons. Thema war die Meldepflicht bei Datenschutzverletzungen. Zudem nahm die FDS am Schulungs-Programm der Staatskanzlei für die KV-Lernende teil.

## 10 Personelles und Ressourcen

Im Berichtsjahr verliess der juristische Mitarbeiter die FDS, er war in einem 40-Prozent-Pensum tätig. Er wollte wegen familiärer Pflichten seine zwei kleinen Teilpensen an verschiedenen Orten aufgeben und an einem Ort in einem höheren Pensum arbeiten. Dies war bei der FDS leider nicht möglich. Aufgrund des Weggangs erhöhte die bisherige juristische Mitarbeiterin ihr Pensum auf 80 Prozent. Wie bereits im Vorjahr verfügt die FDS über 170 Stellenprozente im juristischen Bereich. Neu hat die FDS Budget für eine IT-Audit-Stelle erhalten, das Rekrutierungsprozedere läuft derzeit.

Nicht nur das Aufgabenspektrum der FDS erweiterte sich in den letzten Jahren, sondern es gab auch eine Verschiebung bei den bisherigen Aufgaben: Während einigen Jahren war die Bearbeitung von Einzelfällen die zentrale Aufgabe, auch was die zeitliche Beanspruchung betraf. Nun ist sie nur noch eine Aufgabe unter vielen. Das macht sich bei der Anzahl Geschäftseingänge bemerkbar: Es sind nicht mehr zahlreiche Einzelfälle, die eingehen, sondern in der Anzahl deutlich weniger, aber sehr komplexe Geschäfte. Das ist durchaus im Sinn des Datenschutzes, handelt es sich dabei doch um wichtige Themen, die zahlreiche Personen betreffen. Somit entfalten sie auch eine grössere Wirkung, etwa bezüglich der Sensibilisierung. Anderseits beanspruchen sie die Ressourcen der FDS über viel längere Zeit, einerseits aufgrund der Komplexität, anderseits müssen die Vorhaben teilweise in Etappen beurteilt werden.

## 11 Prüfprogramm 2023

Die FDS legt für das Jahr 2023 folgendes Prüfprogramm fest:

- Pensionskasse
- Geoportal
- Pupil App (Messenger)
- Zugriffe auf kantonale Einwohnerdatenplattform
- Arbeitsbesuch bei einer Gemeindefachstelle für Datenschutz

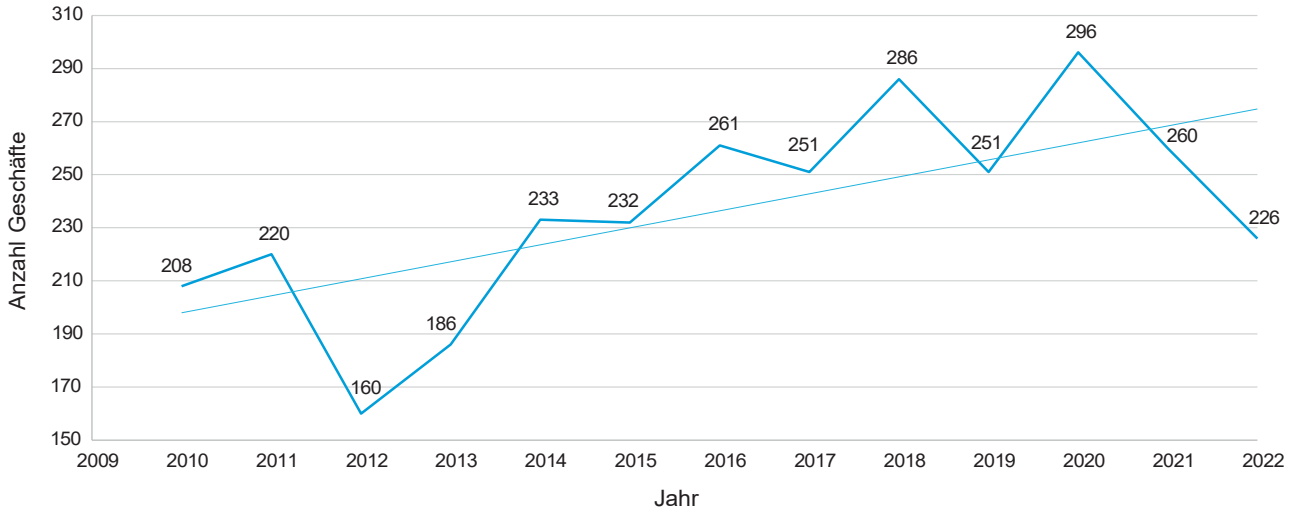
## 12 Antrag

Wir beantragen Ihnen, Herr Präsident, sehr geehrte Damen und Herren, auf den vorliegenden Bericht einzutreten.

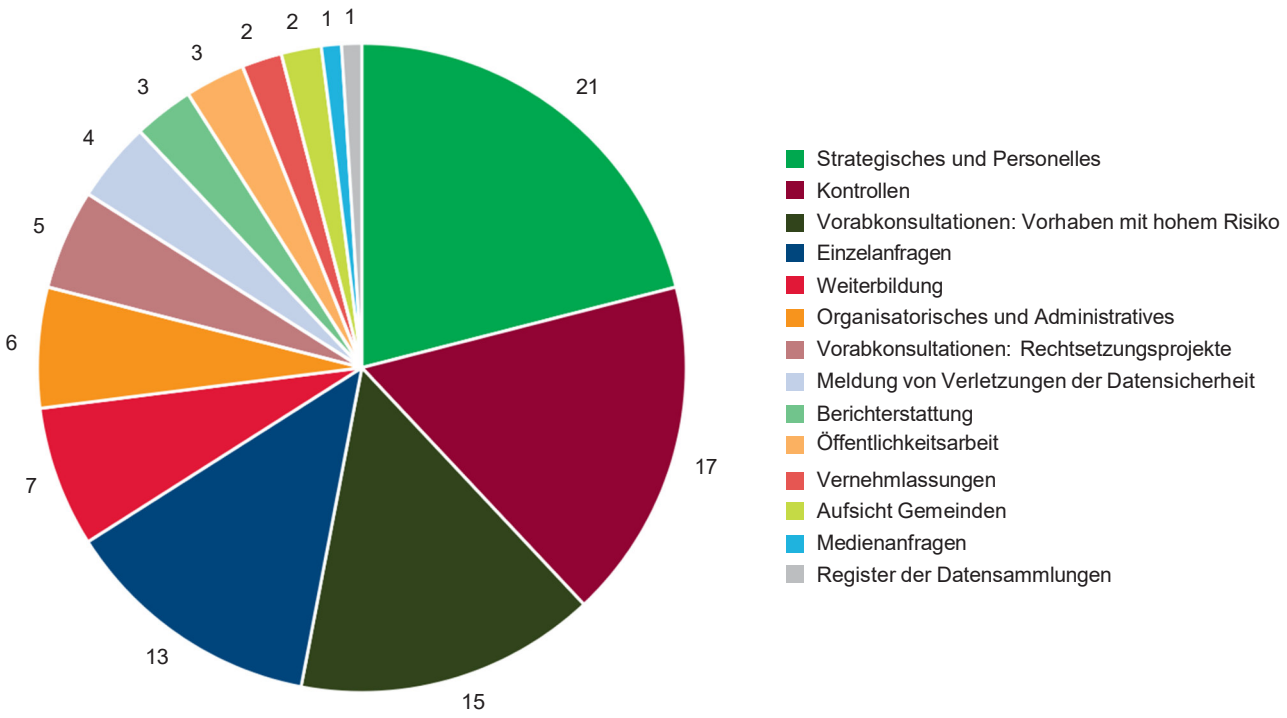
**Kantonale Fachstelle für Datenschutz**

Corinne Suter Hellstern, Leiterin

## Geschäftseingänge




## Aufgabenverteilung nach Art in Prozent



Kantonsrat des Kantons St.Gallen
Geschäft 32.23.03

Fachstelle für Datenschutz
Regierungsgebäude, 9001 St.Gallen
Telefon: 058 229 14 14
E-Mail: datenschutz@sg.ch
Internet: www.datenschutz.sg.ch