Kanton St.Gallen
Fachstelle für Datenschutz

Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2025

Inhaltsverzeichnis

Zusammenfassung

Im Jahr 2025 prüfte die Fachstelle für Datenschutz (FDS) ein Klientinnen- und Klienteninformationssystem und eine Schulverwaltungslösung. Beim Klientinnen- und Klienteninformationssystem CONNET fehlte ein Auftragsdatenbearbeitungsvertrag. Zudem hat der Auftragsdatenbearbeiter einen sehr weitgehenden Zugriff auf das System. Auch auf archivierte Akten darf nur Zugriff haben, wer ihn benötigt. Für alle Institutionen, die CONNET nutzen, braucht es verbindliche datenschutzrechtliche Vorgaben. Erforderlich sind regelmässige Penetrationstests. Logfiles sollten spätestens nach einem Jahr gelöscht werden. Ein Testen mit produktiven Personendaten ist nicht erforderlich und es muss sichergestellt werden, dass die Personendaten wirklich anonymisiert sind.

Beim Schulverwaltungssystem NESA ist die elektronische Archivierung teilweise noch nicht geregelt. In diesem Zusammenhang müssen auch die Verantwortlichkeiten zwischen Schulen und Betriebsleitung geklärt werden. Die Zugriffsrechte im Bereich Statistik und Revision Finanzen beurteilte die FDS unterschiedlich. Weitere Kritikpunkte betrafen Freitextfelder, unverschlüsselte Backups bzw. zu lange Aufbewahrung und Tests mit produktiven Personendaten. Auch wenn es kein spezifisches Thema von NESA ist: Der allgemeine Bildungsauftrag ist keine genügende gesetzliche Grundlage.

Beim Schengener Informationssystem (N-SIS) zeigte die Logfile-Kontrolle bei der Kantonspolizei grundsätzlich korrekte, begründbare Abfragen. Einzelne Abfragen lagen aber in einem Graubereich, etwa ausserhalb der Arbeitszeit. Die FDS empfahl, regelmässig zu schulen und daran zu erinnern, dass Abfragen nur dienstlich und grundsätzlich während der Arbeitszeit erfolgen.

Der FDS wurde ein Diebstahl von Kameras mit Speicherkarten gemeldet. Es stellte sich die Frage, wie das Risiko einzuschätzen sei. Weil Daten unter einem Berufsgeheimnis betroffen waren und es sich um einen Diebstahl handelte, bewertete die FDS das Risiko als hoch. Nach weiteren Abklärungen durch die Institution zeigte sich, dass Personen nicht identifizierbar waren. Der Fall war somit nicht meldepflichtig. Dieses Beispiel zeigt, wie wichtig eine gründliche Abklärung ist.

Auf Gemeindeebene war die zukünftige Organisation der Gemeindefachstellen Thema. Neu bietet die Stadt St.Gallen an, die Funktion der Datenschutzstelle für Gemeinden zu übernehmen. Die Fachstelle Rheintal Werdenberg Sarganserland führt ihre Aufgabe weiter. Ein Arbeitsbesuch bei letzterer zeigte stabile Strukturen und erfüllte Unabhängigkeit, aber auch die Notwendigkeit, bei Prüfungen bei Bedarf IT-Kompetenz beizuziehen und stete Weiterbildung sicherzustellen.

Die FDS prüfte ein Reglement zur Videoüberwachung: Zweck und Verantwortlichkeiten waren zu wenig klar geregelt. Die Regelung von Protokollierung der Zugriffe, Hinweisschilder vor Ort, automatische Löschung und kurze Aufbewahrung sind wichtig. Tonaufnahmen erachtet die FDS grundsätzlich als unverhältnismässig.

Es gingen wesentlich mehr Anzeigen ein als im Vorjahr. Teilweise beanspruchten sie die FDS stark, weil die Erledigung oder sogar die Mitteilung der Unzuständigkeit nicht akzeptiert wurde. Inhaltlich befasste sich die FDS mit der Datenbearbeitung in einem Gremium und einer Anzeige zur Einwilligung für unverschlüsselten E-Mail-Versand.

Die Einzelanfragen betrafen u.a. Stimmregister, Strafregisterauszüge, Bearbeitung von Personendaten von Bewerberinnen und Bewerbern sowie Verschlüsselung von Pager-Nachrichten.

Ab 1. Januar 2026 gilt die Vereinbarung für die Zusammenarbeit der Datenschutzbehörden der Kantone St.Gallen, Thurgau sowie Appenzell Innerrhoden und Ausserrhoden. Das Plenum der Vereinigung der schweizerischen Datenschutzbeauftragten fand in St.Gallen statt. Die Ressourcenlage bleibt angespannt: Das Team ist klein, die Stellenprozente bleiben gleich, während Geschäftseingänge und Komplexität weiter steigen und einzelne Fälle überdurchschnittlich viel Zeit binden.

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 2025.

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.

1 Einleitung

Das Jahr 2025 zeichnete sich nicht durch ein einzelnes prägendes Thema aus wie in Vorjahren etwa die Videoüberwachung oder M365. Die FDS bearbeitete vielfältige Themen: Sie prüfte ein Klientinnen- und Klienteninformationssystem und die Abfragen auf das Schengener Informationssystem, nahm Stellung zu einem Videoüberwachungsreglement, koordinierte sich mit der Gemeindeaufsicht und befasste sich mit der Reorganisation der Gemeindefachstellen für Datenschutz. Die FDS verzeichnete eine Zunahme der Geschäftseingänge von beinahe einem Fünftel. Wie bereits in der Vergangenheit erwähnt, sind es die grossen, sehr komplexen Geschäfte wie die Vorabkonsultationen oder Prüfungen, welche viel Zeit benötigen.

Die mit der Revision des Datenschutzgesetzes 2019 eingeführten Instrumente – Datenschutz-Folgenabschätzung und Meldung der Verletzung der Datensicherheit – haben dazu geführt, dass Datenschutz in den Geschäfts-Prozessen berücksichtigt wird. Die öffentlichen Organe setzen sich so frühzeitig mit dem Thema auseinander. Die FDS ist der Ansicht, dass damit das Bewusstsein für den Datenschutz gestiegen ist. So ist etwa festzustellen, dass Auftragsdatenbearbeitungsverträge meistens vorhanden sind. Das war vor ein paar Jahren noch nicht der Fall. Auch haben viele öffentliche Organe Datenschutzberaterinnen oder -berater ernannt: Bei der Staatskanzlei berät seit drei Jahren die Stelle IT-Recht und Datenschutz die Stellen der kantonalen Verwaltung. E-Government St.Gallen digital verfügt seit dem Berichtsjahr ebenfalls über eine Datenschutzberatung. Diese niederschwelligen Anlaufstellen helfen, ein gutes Datenschutz-Niveau zu erreichen. Ein weiteres Zeichen für ein erhöhtes Bewusstsein sind öffentliche Organe, die sich bei der FDS melden und mitteilen, dass sie auf die Bearbeitung in der vorgesehenen Microsoft Cloud verzichten und nach einer Alternative suchen würden. Vielen öffentlichen Organen ist vermehrt bewusst, dass sie auch im Fall einer Datenschutzverletzung verantwortlich bleiben. Nichtsdestotrotz gibt es Themen, die vermehrt beachtet werden sollten: Bei der Archivierung stellt die FDS immer wieder Mängel fest. Sei es, dass die elektronische Archivierung bei neuen Projekten noch nicht angegangen wurde oder dass die Zugriffsberechtigungen auf archivierte Akten zu weit sind. Auch die Rechtsgrundlagen genügen für die Vorhaben nicht immer. Teilweise sind (noch) gar keine vorhanden, oder die vorhandenen sind nicht genügend bestimmt. Ein oft diskutiertes Thema sind Zugriffsrechte auf Systeme. Ein gutes Management der Zugriffsrechte ist für die Einhaltung des Datenschutzes zentral. Auch der Umgang mit Logfiles und Backups sind häufig Thema. In beiden Fällen müssen Aufbewahrung, Zugriffsrechte und Verschlüsselung geregelt werden.

2 Prüftätigkeit

2.1 Klientinnen- und Klienteninformationssystem

Im Berichtsjahr schloss die FDS die Prüfung des Klientinnen- und Klienteninformationssystems CONNET ab. CONNET dient dazu, Personen in Jugendeinrichtungen und Einrichtungen für erwachsene Personen mit einer Behinderung zu erfassen, Kostenübernahme-Garantien zu bearbeiten und die Aufenthalte abzurechnen. Aufgrund der Umstellung des Finanzierungssystems im Bereich Behinderung ergeben sich neue Anforderungen an die Funktionalitäten von CONNET.

Entwicklung der Fachanwendung und Support übernimmt eine externe Stelle. Dabei fehlte der Auftragsdatenbearbeitungsvertrag. Die FDS empfahl, rasch eine Vereinbarung abzuschliessen. Der Dritte hat zudem vollständigen und zeitlich unbegrenzten Zugriff auf das System. Die FDS empfahl zu prüfen, ob ein derart weiter Zugriff erforderlich ist.

Nebst dem zuständigen Amt nutzen auch Einrichtungen für Personen mit Behinderung CONNET. Im Zusammenhang mit der Nutzung von CONNET ist das zuständige Amt verpflichtet, den Einrichtungen entsprechende Vorgaben zu machen, welche die Einhaltung der Datenschutz-Bestimmungen betreffen. Personen dürfen nur auf diejenigen Daten ihrer Institution Zugriff haben, die sie für ihre Aufgabenerfüllung benötigen. Zudem dürfen nur persönliche Zugänge verwendet werden.

Die Fachstelle für Statistik hat für die Erstellung von Statistiken Zugriff auf die Daten in CONNET. Dabei handelt es sich um einen ständigen Zugriff im Abrufverfahren. Weil die Datenbekanntgabe im Abrufverfahren eine Rechtsgrundlage benötigt, empfahl die FDS, eine solche zu schaffen. Einen ständigen Zugriff erachtet die FDS als nicht verhältnismässig.

Auf archivierte Akten dürfen nur diejenigen Personen Zugriff haben, welche sie für ihre gesetzliche Aufgabenerfüllung benötigen. Werden sie in einem Raum aufbewahrt, zu dem auch andere Organisationseinheiten Zutritt haben, müssen sie in abgeschlossenen Schränken aufbewahrt werden. Dasselbe gilt auch für laufende Dossiers. Die elektronische Archivierung muss noch geregelt werden. Bisher werden sämtliche Dossiers aufbewahrt, auch wenn eine Person in einen anderen Kanton wechselt oder austritt. Eine «ewige» Aufbewahrung ist datenschutzrechtlich ohne gesetzliche Grundlage nicht zulässig. Die Frage der Aufbewahrungsfrist bemisst sich nach den Rechtsgrundlagen und danach, während welcher Dauer die Daten für die gesetzliche Aufgabenerfüllung unentbehrlich sind. Danach müssen die Dokumente dem Staatsarchiv angeboten bzw. vernichtet werden.

Die FDS empfahl, einen Penetrationstest[4] durchzuführen. Dieser dient dazu, potentielle Sicherheitsrisiken frühzeitig zu entdecken und zu beheben. Er sollte in regelmässigen Zeitabständen oder bei grösseren Veränderungen in der IT-Infrastruktur durchgeführt werden.

Die Logfiles wurden bisher nicht gelöscht. Mit Logfiles können Veränderungen am oder Zutritte zum System aufgezeichnet werden. Dadurch kann identifiziert werden, wer wann auf das System zugegriffen hat. Besonders nach einem IT-Sicherheitsvorfall sind Logfile-Auswertungen von grosser Bedeutung, um den Sachverhalt rekonstruieren zu können. Die Aufbewahrung von Logfiles auf unbestimmte Dauer ist aber weder notwendig noch datenschutzkonform. Logfiles sollten spätestens nach einem Jahr gelöscht werden.

Für das Testen im neuen System werden Datensätze des derzeit produktiven Systems «verfälscht»: Es werden Bestandteile der Datensätze entnommen und bei anderen Datensätzen eingesetzt, so dass nicht mehr die ursprünglichen Datensätze bestehen. Die FDS erachtet dieses Vorgehen als heikel. Das «Verfälschen» der Daten bewirkt nicht zwingend eine Anonymisierung. Das muss aber sichergestellt werden. Im vorliegenden Fall ist es nicht notwendig, dass mit produktiven Daten getestet wird. Für das Testsystem muss derselbe technische und organisatorische Schutz gelten wie für die produktiven Personendaten ausserhalb des Testsystems.

Des Weiteren machte die FDS Empfehlungen zur Definition von Prozess und Verantwortlichkeit im Fall einer Verletzung der Datensicherheit und zur Gewährung der Rechte der betroffenen Personen, zur Schulung und Sensibilisierung,

Die zuständige Stelle hat die meisten Empfehlungen angenommen und teilweise bereits umgesetzt.

2.2 Schulverwaltungssoftware

Nesa ist eine Schulverwaltungssoftware für die kantonalen Mittelschulen und Berufsfachschulen. Damit werden die für die Schulverwaltungsprozesse benötigten Personendaten von Schülerinnen und Schülern, Lehrpersonen sowie Verwaltungsangestellten bearbeitet. Inskünftig sollen in Nesa auch besonders schützenswerte Personendaten wie Arztzeugnisse, disziplinarische Massnahmen, Nachteilsausgleich und Coachingprotokolle von Lernenden bearbeitet werden. Die FDS hat Nesa bereits im Jahr 2017 geprüft.

Auch wenn es kein spezifisches Problem von Nesa ist, äusserte sich die FDS zur Rechtsgrundlage. Nach ihrer Ansicht muss die Bearbeitung von Personendaten im Schulbereich generell in den Grundzügen in einem formellen Gesetz geregelt werden. Der allgemein formulierte Bildungsauftrag ist keine hinreichend bestimmte Norm für die Bearbeitung insbesondere von besonders schützenswerten Personendaten. Dazu äusserte sich die FDS bereits früher.[5]

4 Umfassender Sicherheitstest einzelner Rechner, Netzwerke oder Anwendungen (aus Wikipedia, 2. Februar 2026).

5 Siehe Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2022, S. 13, 2024 S. 8.

Derzeit nur teilweise bzw. bei einzelnen Schulen geregelt ist die elektronische Archivierung. Die Umsetzung dieses Punktes muss rasch anhand genommen werden. Die Verantwortlichkeiten zwischen den Schulen und dem Betriebsleiter Nesa müssen festgelegt werden.

Ein anderes besprochenes Thema waren die Zugriffsrechte der Revisorinnen und Revisoren der Finanzkontrolle und der Fachstelle für Statistik. Beide Stellen haben einen dauernden Zugriff auf die Personendaten in Nesa, allerdings mit unterschiedlichen Berechtigungen was den Umfang der Daten anbelangt. Die Fachstelle für Statistik hat aufgrund ihrer Aufgabenerfüllung im Rahmen der Bundesstatistik Zugriff. Die FDS erachtet diesen sowohl bezüglich der erforderlichen Rechtsgrundlagen als auch der Verhältnismässigkeit als rechtmässig. Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht unentbehrlichen Daten einschliesslich besonders geschützter Personendaten aus den Datensammlungen der Dienststellen einzusehen. Allerdings fehlt die gesetzliche Grundlage für die Datenbekanntgabe im Abrufverfahren. Eine solche sollte geschaffen werden. Zudem sollte der Zugriff zeitlich eingeschränkt werden, weil er nur punktuell im Rahmen der Prüfungstätigkeit erforderlich ist.

Innerhalb der Anwendung gibt es Freitextfelder, etwa im Modul «Absenzen». In diese Felder können Benutzende unstrukturiert beliebige Informationen eingeben. Freitextfelder sollten aus datenschutzrechtlicher Sicht vermieden werden. Ist das nicht möglich, muss die Rechtmässigkeit der Eingaben regelmässig überprüft werden.

Empfehlungen machte die FDS zu den Backups: Sie sollen nicht länger als ein Jahr aufbewahrt werden, ältere Backups müssen sofort vernichtet werden. Zudem müssen sie verschlüsselt aufbewahrt werden. Die Zugriffsrechte müssen so eingeschränkt werden, dass nur diejenigen Personen, die einen Restore machen müssen, Zugriff haben.

Sicherheitskontrollen sollten in regelmässigen, kürzeren Zeitabständen durchgeführt werden, insbesondere auch angesichts des raschen technologischen Wandels. Nach grundlegenden Änderungen in der Anwendung sollte jeweils grundsätzlich ein Penetrationstest durchgeführt werden. Wichtig ist, dass die Ziele genau definiert und mit der externen Firma abgestimmt werden.

Logfiles beinhalten detaillierte Ereignisdaten (Zeitstempel, aufgerufene Funktionen, Dateioperationen). Daraus lassen sich präzise Benutzeraktivitäten und Verhaltensmuster ableiten. Ohne gezielte Zugriffsbegrenzung besteht somit das Risiko einer unerlaubten Überwachung oder eines Missbrauchs dieser sensiblen Informationen. Die Zugriffsrechte auf die Logaktivitäten müssen deshalb angemessen eingeschränkt werden.

Tests in Nesa finden mit produktiven Personendaten statt. Dies widerspricht dem Grundsatz der Zweckmässigkeit. Auch ist für die FDS nicht ersichtlich, weshalb es für das Testen Personendaten benötigt. Anonymisierte Daten würden genügen. Zudem handelt es sich um sensible Daten: In Nesa werden mit den Schülerdaten sensible (neu besonders schützenswerte) Personendaten von meist Minderjährigen in einem Abhängigkeitsverhältnis bearbeitet. Auch die Personen in einem Anstellungsverhältnis sind in einem Abhängigkeitsverhältnis.

Weitere Empfehlungen betrafen die Auftragsdatenbearbeitung, die Schulung und Sensibilisierung, den Prozess zur Meldung einer Datenschutzverletzung, die Stellvertretung und unpersönliche Accounts.

Die zuständige Stelle hat die meisten Empfehlungen angenommen und teilweise bereits umgesetzt.

2.3 Publikationsplattform

Die FDS prüfte die kantonale Publikationsplattform, auf der die amtlichen Publikationen veröffentlicht werden. Anlass waren mehrere Anzeigen von Bürgerinnen und Bürgern sowie eigene Stichproben. Es ging darum, dass Publikationen mit Personendaten teilweise länger online abrufbar waren als für den Publikationszweck erforderlich.

Die Prüfung fokussierte sich auf die amtlichen Bekanntmachungen von Kanton und Gemeinden im Amtsblatt. Die FDS stellte fest, dass eine technische Koppelung von Rubriken und Löschfristen fehlt. Auf der Plattform sind Rubriken im Amtsblatt nicht mit verbindlichen Löschfristen verknüpft. Dadurch fehlt eine automatisierte Kontrolle, wann Publikationen ausgeblendet bzw. gelöscht werden müssen. Es erhöht sich das Risiko, dass Personendaten zu lange in der Publikationsplattform verfügbar sind. Zudem entsteht Aufwand für die manuelle Prüfung und Löschung.

Die FDS empfahl für Rubriken, die Personendaten beinhalten, Löschfristen festzulegen und technisch im System zu hinterlegen. Zudem soll die Plattform Publikationen nach Ablauf der Frist automatisch ausblenden oder löschen.

Die zuständige Stelle hat die Empfehlungen angenommen und teilweise bereits umgesetzt.

2.4 Schengener Informationssystem

Als kantonale Aufsichtsbehörde ist die FDS gesetzlich verpflichtet, regelmässige Kontrollen bei den kantonalen öffentlichen Organen durchzuführen, welche auf den nationalen Teil des Schengener Informationssystems (N-SIS) Zugriff haben. Im Berichtsjahr führte die FDS eine Kontrolle bei der Kantonspolizei durch. Die Prüfung fand in Form einer Logfile-Kontrolle statt. Prüfungsgegenstand waren die Nutzung des N-SIS und das Datenschutzbewusstsein der Mitarbeitenden.

Die FDS stellte fest, dass die Nutzung des N-SIS unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgt. Im Rahmen der Stichprobenkontrolle konnten sämtliche Abfragen mit der Aufgabenerfüllung der befragten Person begründet und anhand der Einträge in der elektronischen Geschäftskontrolle erläutert werden. Ein paar Abfragen ergingen in einem Graubereich: Mitarbeitende tätigten Abfragen aufgrund von ausserhalb der Arbeitszeit gemachten Wahrnehmungen; oder die Abfragen wurden ausserhalb der Arbeitszeit gemacht. Der Übergang zu einer unzulässigen Abfrage ist fliessend. Die FDS empfahl, die Mitarbeiterinnen und Mitarbeiter periodisch daran zu erinnern, dass Abfragen grundsätzlich während der Arbeitszeit und ausschliesslich zu dienstlichen Zwecken erfolgen müssen. Zudem sollen die Mitarbeiterinnen und Mitarbeiter bei Eintritt in der Nutzung der Systeme sowie im Umgang mit Personendaten allgemein geschult werden. Danach soll zusätzlich zum erwähnten E-Learning wiederkehrend spezifisch auf datenschutzrechtliche Fragestellungen im Kontext der Polizeiarbeit hin sensibilisiert werden.

Die zuständige Stelle hat die Empfehlungen angenommen und teilweise bereits umgesetzt.

2.5 Zugriffe auf kantonale Einwohnerdatenplattform

Die FDS hat im Berichtsjahr die stichprobeweise Kontrolle der Zugriffe auf die kantonale Einwohnerdatenplattform bei einer Stelle im Justiz- und Sicherheitsdepartement geprüft. Die Ergebnisse werden im Verlaufe des Jahres 2026 vorliegen.

2.6 Klinikinformationssystem

Ende des Berichtsjahres prüfte die FDS das Klinikinformationssystem (KISIM) bei einem Spital. Die Prüfung wird im Jahr 2026 abgeschlossen.

3 Meldungen Verletzung Datensicherheit

3.1 Diebstahl Kamera

Eine Meldung betraf die Entwendung von zwei Kameras mit Speicherkarten. Die Räumlichkeiten waren nur mit einem Badge zugänglich. Die Speicherkarten beinhalteten nach Angaben des öffentlichen Organs Daten von rund 200 Personen.

Das öffentliche Organ wandte sich mit der Frage an die FDS, wie sie das Risiko einschätze. Eine Meldung einer Verletzung der Datensicherheit ist dann erforderlich, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Person führt. Die FDS stufte die Verletzung als voraussichtlich hohes Risiko ein. Dies aufgrund folgender Überlegungen: Es sind Personendaten unter einem Berufsgeheimnis betroffen. Sie wurden aus einem abgeschlossenen Raum gestohlen und nicht liegengelassen oder verloren. Die FDS geht im Fall eines Diebstahls von einem höheren Risiko aus, weil nicht auszuschliessen ist, dass sich das kriminelle Verhalten auch auf die Personendaten auswirken könnte. Ein nicht näher begründetes subjektives Vertrauen in gute Absichten von unbekannten Datenempfängern vermag ein objektiv hohes Risiko nicht auszuschliessen. Bei einem Verkauf an Dritte besteht die Möglichkeit, dass ein Käufer ein Interesse an den Daten haben könnte. Zudem wurde unbemerkt ein Badge einer Mitarbeitenden bzw. eines Mitarbeitenden entwendet. Es fehlten Hinweise, ob er wieder aufgetaucht ist oder nicht.
Das öffentliche Organ machte aufgrund dieser Einschätzung weitere Abklärungen. Diese ergaben, dass nicht abgeleitet werden könne, von wem die Fotos seien, da nur das Datum ersichtlich sei. Somit würde es sich nicht mehr um Personendaten handeln. Eine Meldung an die FDS war demnach nicht erforderlich. Der Fall zeigt, dass es wichtig ist, jeden Vorfall genau abzuklären.

3.2 Privater Export von Geschäftsdaten

Ein Amt hatte den Verdacht, dass ein Mitarbeiter Personendaten aus Dossiers auf eine private Festplatte exportierte. Es handelte sich um besonders schützenswerte Personendaten einer besonders verletzlichen Personengruppe. Der Fall lag bereits ein Jahr zurück, als er entdeckt wurde. Danach machte die Stelle umgehend Meldung.

Das betroffene Amt hatte zum Zeitpunkt der Meldung mehrere Massnahmen umgesetzt, so die Überprüfung aller Zugriffsberechtigungen und wo nötig Einschränkung der zugriffsberechtigten Personen, Schulung und Thematisierung der Löschung von Daten während der Schlussphase und des Austritts («Aufräumaktionen») sowie eine Meldung beim Untersuchungsamt. Die FDS empfahl zudem Logfiles anzufordern, die Rückschlüsse über sämtliche Downloads von einzelnen Mitarbeitenden zulassen. Die Zugriffsrechte sollen in regelmässigen zeitlichen Abständen überprüft und gegebenenfalls den Umständen entsprechend angepasst werden. Eine Sensibilisierung bezüglich des Datenschutzes und der Informationssicherheit sollte regelmässig erfolgen. Der genaue Sachverhalt sollte jeweils möglichst rasch abgeklärt werden. Das ist wichtig sowohl für zu ergreifende Massnahmen als auch die Frage der Information der betroffenen Personen und der Klärung, ob ein hohes Risiko vorliegt.

Die FDS war der Auffassung, dass die betroffenen Personen informiert werden müssen, wenn nach genauer Abklärung des Sachverhalts die Wahrscheinlichkeit gross ist, dass die angestellte Person mit dem Export der zip-Dateien private Zwecke verfolgt. In einem solchen Fall bestehen erhebliche Risiken wie ein möglicher Identitätsdiebstahl. Eine Informationspflicht besteht, wenn die Betroffenen durch die Information die Risiken für ihre Persönlichkeit und Grundrechte reduzieren können. Dies kann auch dann der Fall sein, wenn die betroffenen Personen Vorgänge in ihrem Umfeld mit erhöhter Aufmerksamkeit verfolgen und somit besser einordnen können, um notwendige Handlungen vorzunehmen. Gegen eine Information könnte eingewendet werden, dass der Vorfall bereits mehr als ein Jahr zurückliegt und dass mit zunehmender Zeitdauer seit dem Ereignis die Wahrscheinlich abnehmen dürfte, dass damit zusammenhängende Vorkommnisse geschehen. Allerdings ist diesem Kriterium kein allzu hohes Gewicht beizumessen; ansonsten bestünde die Gefahr, dass Meldung oder Abklärung von Sachverhalt verzögert würden, um nicht informieren zu müssen.

4 Aufsicht und Beratung Gemeindefachstellen für Datenschutz

4.1 Zukünftige Organisation

Das DSG sieht vor, dass die Gemeinden eigene Datenschutzbehörden einsetzen. Sie sind für die Organisation selbst verantwortlich. Derzeit gibt es drei regionale Gemeindefachstellen für Datenschutz und diejenige der Stadt St.Gallen. Der Verband St.Galler Gemeindepräsidien (VSGP), als Trägerverein der politischen Gemeinden, beabsichtigte, die heutige Organisation zu ändern. Das Vorhaben kam nicht zustande und der VSGP zog sich aus der zukünftigen Organisation der Gemeindefachstellen für Datenschutz zurück. Vorgesehen ist nun folgendes Modell: Die Stadt St.Gallen hat den Gemeinden angeboten, eine Vereinbarung mit ihnen abzuschliessen. Die städtische Fachstelle für Datenschutz würde die Funktion dann nicht nur für die Stadt, sondern auch für die Vereinbarungsgemeinden übernehmen. Einige Gemeinden aus den Regionen Oberuzwil und Rapperswil-Jona haben sich dafür entschieden. Die Gemeinden der Region Rheintal Werdenberg Sarganserland verbleiben bei der bisherigen Fachstelle. Die Stellenleitung der Fachstelle für Datenschutz der Stadt St.Gallen wird derzeit ad interim geführt. Die bisherige Stelleninhaberin hat per Anfang Oktober 2025 eine neue berufliche Herausforderung angenommen.

Als Aufsichtsorgan hat sich die FDS zu den Leitplanken für die zukünftige Organisation der Aufsichtsbehörden bereits im letzten Tätigkeitsbericht geäussert:[6] Die Stellen müssen in ihrer Aufgabenerfüllung unabhängig sein und über genügend Ressourcen verfügen. Die FDS schätzt, dass diese für die Gemeinden etwa 200 bis 250 Stellenprozente betragen sollten. Diese Schätzung umfasst auch Know-how im IT-Bereich und die Stellvertretung. Eine Konzentration dürfte zu einer Professionalisierung führen. Angesichts der weiter zunehmenden Komplexität ist das zu begrüssen. Auch dürfte dadurch die Unabhängigkeit gestärkt werden, wenn nebenbei nicht noch andere Aufgaben, auch wenn sie vereinbar sind, erfüllt werden.

6
Tätigkeitsbericht 2024, S. 14.

4.2 Aufsicht Amt für Gemeinden

Die Gemeinden sind wie erwähnt verpflichtet, eigene Datenschutzstellen einzusetzen. Im Zusammenhang mit der Reorganisation ist es sinnvoll zu kontrollieren, ob die Gemeinden ihrer gesetzlichen Pflicht nachgekommen sind. Die FDS hat deshalb mit der Gemeindeaufsicht Kontakt aufgenommen. Diese nimmt den Punkt in ihr Prüfprogramm auf.

4.3 Arbeitsbesuch

Im Jahr 2024 sah die FDS einen Arbeitsbesuch bei der Fachstelle für Datenschutz Rheintal Werdenberg Sarganserland (FS RWS) vor. Aufgrund der vorgesehenen Reorganisation verzichtete die FDS. Als klar war, dass die FS RWS ihre Funktion weiterhin erfüllen wird, stattete die FDS ihr im Berichtsjahr einen Arbeitsbesuch ab. Was die Organisation und die IT betrifft, hat sich gegenüber dem letzten Besuch im Jahr 2020 nichts verändert. Derzeit verfügt die Stelleninhaberin über ein Pensum von 70 Prozent inkl. Sekretariat. Die Ressourcen können flexibel angepasst werden. Die Voraussetzungen an die Unabhängigkeit erachtet die FDS als erfüllt: Weder ist eine äussere Beeinflussung ersichtlich noch handelt die Stelle weisungsgebunden. Wie bereits im Tätigkeitsbericht des Jahres 2020 ausgeführt[7], ist der Stellenleiter Kantonsrat im Parlament des Kantons St.Gallen. Eine Unvereinbarkeit besteht nicht. Im Einzelfall muss jeweils abgewogen werden, ob ein Ausstandsgrund besteht. Die Stelleninhaberin erfüllt ihre Aufgabe motiviert und engagiert. Die FS RWS nimmt ihre Aufgaben umfassend wahr. Ein Schwerpunkt der Tätigkeit liegt bei den Kontrollen. Die Vereinbarungsgemeinden werden in einem regelmässigen Turnus geprüft. Die FDS erachtet es als wichtig, dass in jedem einzelnen Fall beurteilt wird, ob der Beizug von unabhängigen Stellen mit IT-Know-how auch bei Prüfungen vor Ort notwendig ist. Erfahrungsgemäss erfordern in der heutigen Zeit die meisten Prüfungen einen solchen Beizug. Im Auge zu behalten ist die stark steigende Komplexität der Materie auch auf Stufe Gemeinde. Die stete Weiterbildung ist wichtig, ebenso der Beizug von juristischem Know-how bei Bedarf. Die FDS steht beratend zur Verfügung. Thema war auch die Archivierung bzw. Vernichtung von Unterlagen. Die FDS hat angeregt, das mit der zuständigen Gemeinde zu klären.

7 S. 12.

4.4 Erfahrungsaustausch

Am Austausch der FDS mit den Gemeindefachstellen für Datenschutz war vorab die Reorganisation Thema.

Bisher bestand ein regelmässiger Erfahrungsaustausch der Gemeindefachstellen für Datenschutz mit der kantonalen Fachstelle. Ein regelmässiger Austausch unter den Gemeindefachstellen für Datenschutz fand bisher nicht statt. Die FDS würde einen solchen sehr begrüssen. Die bearbeiteten Themen und Projekte bei den Gemeinden sind häufig gleich oder zumindest vergleichbar. Eine solche regelmässige Zusammenarbeit käme sowohl den Gemeindefachstellen als auch den Gemeinden zugute. Dieses Thema soll besprochen werden, wenn die Stelle bei der Stadt St.Gallen besetzt und die Reorganisation der Datenschutz-Aufsicht auf Gemeindeebene fortgeschritten ist.

5 Rechtsetzung

5.1 Allgemeines

Seit dem Jahr 2019 müssen Rechtsetzungsprojekte, die den Datenschutz betreffen, der FDS zur Vorabkonsultation vorgelegt werden. Es stellte sich die Frage, welche Vorhaben darunterfallen. Gehören Weisungen, Richtlinien oder Merkblätter auch dazu? Zur Vorabkonsultation müssen Vorhaben vorgelegt werden, die rechtsetzenden Charakter haben, unabhängig von der Stufe. Rechtsetzend sind generell-abstrakte Normen, die für eine unbestimmte Zahl von Personen und Fällen verbindlich gelten und Pflichten auferlegen, Rechte verleihen oder Zuständigkeiten festlegen. Ein Merkblatt oder eine Checkliste dürfte tendenziell nicht darunterfallen, da sie üblicherweise nicht rechtsetzend ist. Richtlinien hingegen, die sich etwa verbindlich an das Verwaltungspersonal richten, gehören dazu. Es muss in jedem einzelnen Fall geprüft werden, ob ein Vorhaben rechtsetzend ist.

5.2 Gesetz über die soziale Sicherung und Integration von Menschen mit Behinderung

Der individuelle Unterstützungsbedarf von Menschen mit Behinderung soll erfasst und basierend darauf ermittelt werden, welche Unterstützungsleistungen nötig sind. Dafür war die Schaffung eines neuen Systems geplant. Neu soll die Person mit Behinderung bei der zuständigen kantonalen Stelle einen Antrag zur Bedarfsermittlung stellen und die dafür erforderlichen Unterlagen einreichen. Die Einschätzung des Bedarfs macht eine verwaltungsexterne Organisation. Dazu hat die FDS verschiedene Empfehlungen gemacht: es muss geklärt bzw. vertraglich zugesichert werden, wer im Fall eines Supports auf Daten zugreifen kann. Es müssen sichere Passwörter verwendet und eine Zwei-Faktoren-Authentifizierung eingesetzt werden. Zudem soll eine Zugangskontrolle für Serverräume vorgesehen werden. Werden besonders schützenswerte Personendaten übermittelt, müssen diese verschlüsselt werden.

5.3 Vereinbarung «justitia.swiss»

Für die elektronische Kommunikation in der Justiz soll eine Plattform geschaffen werden. Die Aufgaben sollen einer Körperschaft mit Rechtspersönlichkeit übertragen werden. Zur Gründung der Körperschaft schliessen der Bund und die interessierten Kantone eine Vereinbarung. Für die Datenbearbeitung in dieser Plattform wäre Bundesrecht anwendbar. Die datenschutzrechtliche Aufsicht läge beim eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. Es stellte sich die Frage, ob für eine Aufsicht durch kantonale Datenschutzbehörden noch Raum bleibt: Bei der Bearbeitung von kantonalen öffentlichen Organen gilt das kantonale Datenschutzgesetz und die kantonale Aufsichtsbehörde ist zuständig. Die FDS empfahl, die Prozesse und Abläufe zur Informationssicherheit zu prüfen. Erforderlich ist, eine Datenschutz-Folgeabschätzung durchzuführen. Im Zusammenhang mit der Auflösung der Körperschaft und dem Austritt aus der Vereinbarung fehlten Regelungen, wie mit allenfalls verbleibenden Personendaten auf der zentralen Plattform umzugehen ist.

5.4 Reglement Videoüberwachung

Der Kanton St.Gallen verfügt bisher nicht über eine formell-gesetzliche Rechtsgrundlage für die Videoüberwachung durch kantonale Organe. Videoüberwachung ist deshalb nur in einem sehr eng begrenzten Bereich zulässig. Sie muss für die gesetzliche Aufgabenerfüllung unentbehrlich sein. Für diese Videoüberwachung braucht es ein Reglement. Ein solches beurteilte die FDS und machte verschiedene Empfehlungen: Sie erachtete den Zweck als nicht genügend bestimmt. Die Regelungen zu den Verantwortlichkeiten waren teilweise schwammig. Zudem war nicht geregelt, in welchen Fällen die Bilder ausgewertet werden dürfen. Auch waren dafür zu viele Stellen befugt. Sämtliche Zugriffe müssen protokolliert werden. Hinweisschilder vor Ort sind zwingend, einzig ein Hinweis auf der Homepage genügt nicht. Die Liste mit den Standorten muss integrierender Bestandteil des Reglements sein. Ton-Aufzeichnungen erachtet die FDS grundsätzlich als nicht verhältnis- und somit als nicht rechtmässig. Die Aufbewahrungsfrist erachtete die FDS als zu lang und nicht verhältnismässig. Die Videoaufnahmen müssen zudem automatisch gelöscht werden. Als besonders problematisch erachtete die FDS eine Bestimmung, wonach jede Person eine Videoüberwachung beantragen kann. Bei der beurteilten Videoüberwachung handelte es sich um einen schweren Eingriff in die Grundrechte der betroffenen Personen. Deshalb muss die Antragsbefugnis gebündelt und auf strategischer Ebene angesiedelt sein. Des Weiteren fehlten Bestimmungen zu technischen Fragen, zur Gewährung der Rechte betroffener Personen und zur Kontrolle der rechtmässigen Durchführung. Die Wirksamkeit der Videoüberwachung muss in regelmässigen zeitlichen Abständen evaluiert werden. Auch dazu fehlte eine Regelung. Schliesslich war zu beachten, dass ein Rechtsetzungsvorhaben jeweils vor Erlass der FDS vorgelegt werden muss.

5.5 Verordnungen zum Gesetz über Referendum und Initiative

Im Zusammenhang mit der Verordnung über das E-Login rügte die FDS die Bestimmung zur «automatisierten Videoüberprüfung» als nicht genügend bestimmt. Bei der automatisierten Videoüberprüfung findet die Identitätsprüfung nicht am Schalter, sondern digital statt («Autoidentifikation»). Nicht klar war zudem, wie dieser automatisierte Prozess ausgestaltet sein würde. Ablauf und Grenzen der automatisierten Videoüberprüfung sollen bereits in den Erläuterungen definiert werden. Ausserdem sollen Details zu Voraussetzungen wie Datenarten, Frames, Speicherfristen für Rohvideos und genauen technischen Methoden geregelt werden.

5.6 Gesundheitsgesetz

Das Gesundheitsgesetz soll revidiert werden. Im Entwurf findet sich eine Bestimmung zur Videoüberwachung durch Gesundheitsinstitutionen. Die FDS kritisierte insbesondere die vage Formulierung der Zweckbestimmung sowie die fehlenden Regelungen zur Aufbewahrung und zur Datensicherheit. Der Einsatz von Technologien zur automatisierten Identifikation von Personen sollte direkt im Gesetzestext untersagt werden und nicht bloss in der Botschaft. Des Weiteren machte die FDS Bemerkungen zur Regelung der Früherkennungsprogramme, zur Einwilligung, zur Patientendokumentation und zur Aufbewahrung.

5.7 Weitere

Die FDS nahm zu weiteren kantonalen und ausserkantonalen Erlassen und Vorhaben Stellung:

- Schifffahrtsverordnung
- Interkantonale Vereinbarung elektronischer Datenaustausch im Justizvollzug
- Einführungsverordnung zum eidgenössischen Strassenverkehrsgesetz
- Personalverordnung
- Gesetz über die Verwaltungsrechtspflege / Bau- und Umweltgesetz
- Aktualisierte Handreichung Datenschutz und Informationssicherheit in der Schule
- Gesetz über Niederlassung und Aufenthalt
- Änderung des Regierungs- und Verwaltungsorganisationsgesetzes
- Verordnung über das Informationssystem Strassenverkehrskontrollen
- Verordnung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise
- Follow up Schengen Evaluation
- Bundesgesetz über Kommunikationsplattformen und Suchmaschinen

6 Vorhaben mit hohem Risiko

6.1 KI im Hochschulbereich

Eine Hochschule plante, einige Tätigkeiten durch eine KI-Lösung erledigen zu lassen; beispielsweise die Erstellung von Verträgen oder die Bearbeitung von rechtlichen Fragestellungen oder Rechtsfällen. In der Lösung würden u.a. besonders schützenswerte Personendaten bearbeitet, die als vertraulich bis geheim eingestuft wurden. Die Hochschule skizzierte unterschiedliche Szenarien: On-Premise-Lösung, Verwendung von Azure innerhalb der Schweiz oder Nutzung EU-Cloud-Anbietern sowie Verwendung eines beliebigen Cloud-Anbieters. Die Hochschule hat das Vorhaben inzwischen nicht mehr weiterverfolgt. Dennoch sollen im Folgenden die Erwägungen der FDS dargelegt werden, da sie von allgemeinem Interesse sind:

Die FDS stellte fest, dass die vorhandenen Rechtsgrundlagen für die vorgesehene Bearbeitung durch eine KI-Lösung in einer Cloud nicht ausreichten. Auch dürfe die KI-Lösung nur unterstützend zum Einsatz kommen. Personendaten dürfen nicht zu Trainingszwecken für andere KI-Modelle verwendet werden. Wichtig ist zu beachten, dass mit der neuen technischen Lösung nicht mehr Personendaten bearbeitet werden dürfen, als bislang für die gesetzliche Aufgabenerfüllung benötigt wurden. Die Einwilligung im Einzelfall ist lediglich für Fälle einer einmaligen Datenbearbeitung in einem konkreten Fall vorgesehen. Umfassende oder regelmässige Bearbeitungen bedürfen einer Grundlage im Gesetz und stellen keinen Einzelfall mehr dar. Eine Einwilligung muss stets freiwillig erfolgen. Freiwilligkeit liegt etwa dann nicht vor, wenn zu verschiedenen Datenbearbeitungen nicht separat eine Einwilligung erteilt werden kann, obwohl dies aufgrund der Unterschiedlichkeit der Sachverhalte angebracht wäre. Zur Anonymisierung und De-Anonymisierung der On-Premise-Anwendung konnten keine konkreten Aussagen getroffen werden, da keine ausreichende Dokumentation über die technische Funktionsweise vorlagen. Damit war es nicht möglich zu bewerten, ob die eingesetzten Verfahren technisch ausgereift sind oder ob beispielsweise durch Kontextwissen dennoch Rückschlüsse auf Personen gezogen werden können.

Aufgrund dieser Feststellungen kam die FDS zum Schluss, dass nur die On-Premise-Lösung eingesetzt werden dürfe. Sofern eine vollständige und vorgängige Anonymisierung der Dokumente möglich wäre und damit ein Personenbezug vollkommen ausgeschlossen werden könne, wären nebst der On-Premise-Lösung auch die anderen Lösungen denkbar.

6.2 Cloudbasierte Plattform im Gesundheitsbereich

Ein öffentliches Organ beabsichtigte für die Mitwirkung der Patientinnen und Patienten und das Management von Krankheits-Symptomen eine cloudbasierte Plattform zu schaffen. Damit sollten u.a. besonders schützenswerte Personendaten in der Azure-Cloud von Microsoft bearbeitet werden.

Die Bearbeitung soll auf einer Einwilligung basieren und die Teilnahme ist freiwillig. Aber selbst wenn eine Patientin oder ein Patient in eine Datenbearbeitung einwilligen würde, muss für eine regelmässige oder systematische Datenbearbeitung aufgrund des Legalitätsprinzips eine genügend bestimmte Rechtsgrundlage vorhanden sein.

Es wurde nicht dargelegt, welche Alternativen es gäbe. Die FDS empfahl, Alternativen zu prüfen und dies zu dokumentieren. Des Weiteren machte sie Empfehlungen zur Zweckbindung, Transparenz, Aufbewahrung, Bearbeitung durch Dritte und zu technischen Aspekten wie beispielsweise das Einrichten eines Monitorings der Datensicherungen.

6.3 M365

M365 war im Jahr 2024 Thema, als die Regierung entschied, die Cloud-Lösung beim Kanton einzuführen. Die FDS berichtete darüber.[8] Punktuell war M365 auch im Berichtsjahr Thema: Einzelne Stellen wandten sich im Rahmen der Einführung an die FDS. Die FDS verwies jeweils auf den Grundsatzentscheid der Regierung und die entsprechende Verantwortlichkeit. Wichtig zu beachten ist, dass wenn Varianten bei der Umsetzung bestehen, die datenschutzfreundlichste Lösung gewählt wird. In manchen Fällen wie etwa beim Beizug von Subunternehmern hat das öffentliche Organ kaum Spielraum. Die FDS wies bereits in der Vergangenheit darauf hin, dass mit dem Entscheid für M365 ein grosser Kontrollverlust verbunden ist, welcher die Einhaltung der Datenschutzbestimmungen zusätzlich stark erschwert oder verunmöglicht.

6.4 Kurs- und Administrationssoftware

Eine externe Firma reichte für eine kantonale Stelle bei der FDS diverse Unterlagen zur Durchführung einer Vorabkonsultation ein. Es sollte ein bestehendes Kursadministrationssystem durch eine neue Standardsoftware ersetzt werden. Das neue System sollte einerseits die Funktionalität des bisherigen Systems abdecken und anderseits den Stellen zur Verwaltung ihrer Personalbestände, ihrer Einsatzplanung, ihrer Alarmierungsmittel, ihrer Einsatz-Rapportierung, ihrer Besoldung und ihres Materials zur Verfügung gestellt werden. Da das Projekt bereits seit dem Jahr 2024 läuft, führte die FDS keine Vorabkonsultation mehr durch. Der Stelle wurde mitgeteilt, dass zu einem späteren Zeitpunkt eine Kontrolle durchgeführt werden würde. Des Weiteren verwies die FDS darauf, dass Unterlagen vom öffentlichen Organ eingereicht werden müssen und es auch Ansprechperson für die FDS ist. Es bleibt für die Einhaltung des Datenschutzes verantwortlich.

8
Tätigkeitsbericht 2024, S. 15.

7 Anzeigen

7.1 Allgemeines

Insgesamt gingen bei der FDS 15 Anzeigen ein. Das sind deutlich mehr als im Vorjahr (2024: 1). Teilweise war die FDS nicht zuständig, sondern die Zuständigkeit lag bei anderen Datenschutzbehörden oder Institutionen. Einzelne Anzeigen beanspruchten die FDS stark: In diesen Fällen akzeptierten die Personen die Erledigung ihrer Anzeige durch die FDS nicht und wurden immer wieder vorstellig. Teilweise wurde nicht einmal die Mitteilung über die Unzuständigkeit akzeptiert.

Die FDS hat die gesetzliche Befugnis, bei offensichtlich unbegründeten oder unverhältnismässig häufigen Fällen die Kosten den betroffenen Personen zu überbinden oder nicht tätig zu werden. Bisher hat die FDS davon keinen Gebrauch gemacht, wird die Entwicklung aber im Auge behalten und bei Bedarf auf diese Möglichkeit zurückgreifen.

7.2 Auskunftsgesuch

Eine Anzeige betraf ein Auskunftsgesuch nach Datenschutzgesetz. Das öffentliche Organ stellte der betroffenen Person einige Unterlagen nicht zu mit der Begründung, die anbegehrten Akten seien keine öffentlichen Dokumente im Sinn des Öffentlichkeitsgesetzes. Nach Ansicht der FDS war das Gesuch nach dem Datenschutzgesetz zu behandeln. Ein öffentliches Organ muss der betroffenen Person klar mitteilen, dass seiner Ansicht nach dem Auskunftsgesuch vollständig nachgekommen wurde. Auch die Gründe, weshalb ein Auskunftsrecht eingeschränkt oder abgelehnt wird, müssen klar mitgeteilt werden. Dies erfolgt mittels einer Verfügung.

7.3 Datenbearbeitung innerhalb eines Gremiums

Eine Anzeige betraf die Bearbeitung besonders schützenswerter Personendaten innerhalb eines Gremiums. Die Bearbeitung von besonders schützenswerten Personendaten ist u.a. zulässig, wenn sie zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist. Unentbehrlichkeit meint, dass die gesetzliche Aufgabe ohne diese Angaben überhaupt nicht erfüllt werden könnte. Die FDS stellte fest, dass für einige Personen die Kenntnis des behandelten Geschäfts nicht unentbehrlich war für ihre gesetzliche Aufgabenerfüllung. Sie empfahl zu prüfen, inwiefern die internen Abläufe angepasst werden können, damit nur diejenigen Personen Kenntnis einer Sache erhalten, die sie für die gesetzliche Aufgabenerfüllung auch benötigen. Im Falle von nicht bestätigten Sachverhalten sollte eine vorgängige Abklärung durch die Geschäftsführung bzw. einen kleinen Kreis von Personen stattfinden. Zudem soll in einem Gremium, das besonders schützenswerte Personendaten bearbeitet, regelmässig in Bezug auf den Datenschutz und die Informationssicherheit geschult werden.

7.4 Einwilligung unverschlüsselter E-Mail-Versand

Eine Anzeige betraf den unverschlüsselten E-Mail-Versand von Angaben, die einem besonderen Amtsgeheimnis unterstehen. Damit gelten erhöhte Anforderungen an Datenschutz und Datensicherheit. Solche E-Mails müssen verschlüsselt versendet werden. Die betroffene Stelle verwies auf die Einwilligung der betroffenen Person. Die FDS erachtete den Wortlaut der Einwilligung als datenschutzkonform. Bemängelt wurde allerdings der Ort des Hinweises. In der gedruckten Version stand der Hinweis neben dem Text-Feld für die E-Mailadresse. Damit war klar, dass bei Eingabe der E-Mail-Adresse ohne Widerspruch die Korrespondenz unverschlüsselt war. In der elektronischen Variante fand sich der gleiche Hinweis jedoch an einer nicht sofort auffindbaren Stelle. Für eine betroffene Person war damit nicht genügend klar, dass eine E-Mail unverschlüsselt versendet wird, wenn die E-Mailadresse angegeben wird. Aus diesen Gründen empfahl die FDS der Stelle, dies transparenter zu gestalten.

8 Einzelanfragen und Medien

8.1 Allgemeines

Auch im Berichtsjahr bearbeitete die FDS zahlreiche Anfragen. Die FDS beurteilte einige Einwilligungserklärungen. Einwilligungserklärungen können im öffentlichen Recht nur in einem sehr eng begrenzten Bereich zum Tragen kommen. Grundsätzlich gilt für öffentliche Organe das Legalitätsprinzip. Danach bedarf jede Aufgabe bzw. Datenbearbeitung einer Rechtsgrundlage. Weiter meldeten sich mehrere Personen mit Anliegen, bei denen sie selbst tätig werden müssen: Einsichts- und Auskunftsgesuche sowie Gesuche um Datensperre müssen sie selbst bei den zuständigen Stellen einreichen.

Cloud-Lösungen sind immer wieder Thema. Ein öffentliches Organ wollte im Sekretariatsbereich eine Automatisierung einführen. Geplant war der Einsatz von KI, basierend auf der Microsoft Azure Technologie. Die FDS hat darüber berichtet.[9] Nach der Beratung durch die FDS teilte das öffentliche Organ mit, es werde auf die vorgesehene Cloud-Lösung verzichten und nach einer Alternative suchen.

9
Tätigkeitsbericht 2024, S. 22.

Nachfolgend werden Anfragen ausgeführt, die von allgemeinem Interesse sind.

8.2 Stimmregister

Die Schaffung eines stehenden Stimmregisters ist im Zusammenhang mit dem Einsatz von E-Collecting und E-Voting nötig. Das stehende Stimmregister dient dazu, die Stimmberechtigten aller Gemeinden zentral und tagesaktuell zusammenzuführen. Zudem werden die Stimmrechtsausweise für die Bürgerinnen und Bürger zentral generiert. Die FDS regte an, das E-Voting-Anmeldeverfahren einem Penetrationstest zu unterziehen. Zudem stellte sie Fragen zur Verschlüsselung und zu den Zugriffsrechten auf die Backups sowie zu den Zugriffsrechten der externen Supportfirmen.

8.3 Strafregisterauszüge

Eine Stelle gelangte an die FDS mit der Frage, ob für die Beschaffung von Strafregisterauszügen ohne Kenntnis darüber, ob ein Eintrag vorhanden ist, erhöhte Anforderungen gelten. Die FDS bejahte die Frage. Dies mit der Begründung, dass es sich um besonders schützenswerte Personendaten handeln könnte.

8.4 Ideeller Zweck

Ein Verband wollte die Bedürfnisse seiner über 50jährigen Mitglieder eruieren, um Massnahmen für die Rekrutierung erarbeiten zu können. Es stellte sich die Frage, ob eine Adressbekanntgabe dafür zulässig sei. Das DSG sieht eine Bekanntgabe unter anderem der Adresse und des Geburtsdatums vor, wenn die Personendaten ausschliesslich für gemeinnützige oder schutzwürdige ideelle Zwecke verwendet werden. Der Zweck ist nicht gewinnorientiert und kann nach Ansicht der FDS darunter subsummiert werden. Somit ist die Bekanntgabe zulässig.

8.5 Daten von Bewerbenden

Es stellte sich die Frage, ob ein Zugriff der Personalzuständigen auf Bewerberdaten zulässig sei. Ziel war, diese Bewerbenden für allfällige weitere offene Stellen anzusprechen. Nach Ansicht der FDS braucht es dafür die ausdrückliche Einwilligung der Bewerbenden. Die FDS hat empfohlen, dass die Bewerbenden im Sinn eines opt-in ein Häkchen in einem Kästchen setzen können.

8.6 Fallberatung mit Teams

Eine Frage war, ob die Fallberatung im sozialen Bereich mittels Teams von Microsoft zulässig sei. Das ist nur zulässig, wenn keine Angaben zu den betroffenen Personen, über die Fälle bearbeitet werden, gemacht werden. Zu berücksichtigen ist, dass Personen auch aufgrund des Kontextes bestimmbar sein können. Zudem müssen die Daten verschlüsselt werden.

8.7 Verschlüsselung von Nachrichten mittels Pager

Eine Frage betraf die Verschlüsselung von Pagern. Einsatzmeldungen stufte die FDS als besonders schützenswerte Angaben ein. Eine solche Mitteilung kann Gesundheitsdaten beinhalten. Deshalb sollten diese künftig nur noch verschlüsselt versendet werden, selbst wenn der Inhalt der Mitteilung nur selten besonders schützenswerte Personendaten enthält. Eine wirksame Verschlüsselung von mobilen Informatikmitteln ist nicht nur Pflicht, sondern auch technisch eine unabdingbare Massnahme zur Verhinderung von Datenschutzverletzungen. Unverschlüsselte Meldungen lassen sich leicht mitlesen bzw. abfangen. Wichtig sind auch klare Regeln für den Umgang mit Schlüsseln, verlorenen Geräten und Rollenwechseln.

8.8 Medien

Die Berichterstattung im Tätigkeitsbericht 2024 zur Einführung von M365 im Kanton St.Gallen führte zu Beiträgen in verschiedenen Medien (Schweiz aktuell, Watson, inside IT). Weitere Themen waren Videoüberwachung in Gemeinden sowie Datenschutz und Fangewalt.

9 Register und Verzeichnis der Bearbeitungstätigkeit

Die Führung des Registers der Datensammlungen bzw. des Verzeichnisses der Bearbeitungstätigkeit funktioniert in den meisten Fällen gut. Die FDS verzeichnete in diesem Bereich keine nennenswerten Anfragen.

10 Zusammenarbeit

Auf politischer Ebene wird – wie bereits im letzten Tätigkeitsbericht erwähnt - eine engere Zusammenarbeit der Datenschutzbehörden der Kantone St.Gallen, Thurgau und beider Appenzell angestrebt; dies in den Bereichen Digitalisierung und kantonsübergreifende Projekte. Die Vereinbarung läuft ab 1. Januar 2026. Das Steuerungsgremium, bestehend aus den Datenschutzbeauftragten der Kantone, ist zuständig für die Schwerpunkt- und Jahresplanung. Per Mitte 2026 wird das Steuerungsgremium durch eine juristische Mitarbeiterin oder einen juristischen Mitarbeiter unterstützt. Diese Stelle wird beim Kanton Thurgau angesiedelt.

Daneben findet ein regelmässiger Austausch zwischen den Datenschutzbehörden der Kantone Appenzell Innerrhoden und Ausserrhoden, Glarus, Graubünden, Schaffhausen, St.Gallen, Thurgau und der Stadt Winterthur statt.

Die Zusammenarbeit mit privatim (Konferenz der schweizerischen Datenschutzbeauftragten) findet hauptsächlich im Rahmen der Vorstandsarbeit, einer Arbeitsgruppe und an den jährlich stattfindenden Plenen statt. Das Plenum fand im Berichtsjahr in St.Gallen statt. Die Datenschutz-Aufsichtsbehörden tauschten sich über die Bearbeitung von Gesundheitsdaten in der Cloud aus. Sie beschlossen dazu eine Resolution.[10]

10
privatim – Konferenz der Schweizer Datenschutz-Beauftragten

Schliesslich arbeitet die FDS in der Schengen-Koordinationsgruppe mit. Dabei geht es um den Austausch, die Koordination und Zusammenarbeit bei der Aufsicht Schengen zwischen den schweizerischen Datenschutzbehörden.

Die FDS hat einen Leistungsauftrag mit dem katholischen Konfessionsteil und dem Bistum über die Wahrnehmung der Aufgabe der Datenschutz-Fachstelle.

11 Sensibilisierung und Weiterbildung

Wie jedes Jahr war die FDS in der Pilotgruppe des E-Learnings Datenschutz und IT-Sicherheit des Kantons. Zudem erstellte sie verschiedene Merkblätter unter Anderem zu Anzeigen. Des Weiteren führte sie eine Informationsveranstaltung bei Bibliotheken durch.

Im Berichtsjahr hat die FDS den Fragenkatalog für den Self-Check fertiggestellt. Der Self-Check soll den öffentlichen Organen des Kantons St.Gallen ermöglichen, ihre «Datenschutz-Fitness» zu testen. Die öffentlichen Organe des Kantons St. Gallens entscheiden selber, ob und wie sie den Self-Check zur Anwendung bringen. Die Einführung ist im Jahr 2026 vorgesehen.

Mitarbeitende nahmen an Weiterbildungen zu den Themen Cybersicherheit, Gesundheit und Datenschutz, Arbeit und Datenschutz sowie KI teil. Ausserdem liess sich die FDS über Organisation und Arbeit des Rechenzentrums Ostschweiz informieren.

12 Personelles und Ressourcen

Die FDS ist weiterhin ein kleines, gut funktionierendes Team. Das erlaubt ihr, dem umfassenden Aufgabenkatalog in seiner Breite nachzukommen. Bei der Tiefe der Beurteilung müssen aus Ressourcengründen allerdings Abstriche gemacht werden. Die FDS verfügt über gleich viele Ressourcen wie in den vorangegangenen Jahren. Die Geschäftseingänge haben aber nicht nur zahlenmässig stark zugenommen, sondern Komplexität und Ansprüche steigen unaufhörlich. Letzteres zeigt sich etwa daran, dass wenige einzelne Personen die FDS überdurchschnittlich beanspruchen (siehe dazu Ziff. 7.1). Alles zusammen führt die FDS bisweilen an den Rand ihrer Kapazität. Mit 240 Stellenprozenten ist sie auch im interkantonalen Vergleich unterdurchschnittlich dotiert.

Weiter bewährt hat sich die interdisziplinäre Zusammenarbeit im Team. So können Vorhaben sowohl juristisch als auch technisch beurteilt werden. Es ist aber auch möglich, rein technische Prüfungen durchzuführen. So prüfte die FDS – wie oben erwähnt – aufgrund von Anfragen aus der Bevölkerung die Frage der Aufbewahrungsfristen bei der Publikationsplattform.

13 Prüfprogramm 2026

Die FDS legt für das Jahr 2026 folgendes Prüfprogramm fest:

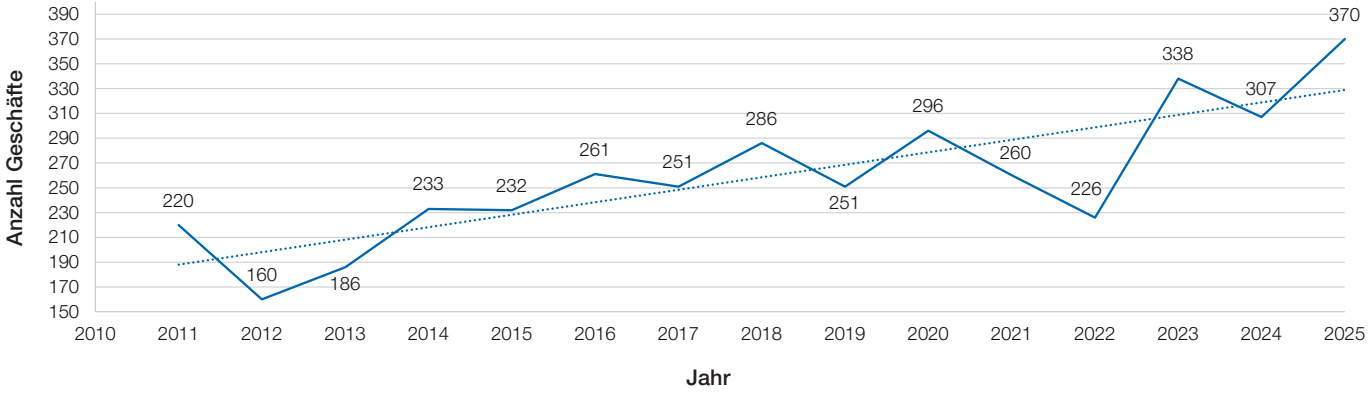
- Kurs- und Administrationssoftware LODUR bei Gebäudeversicherungsanstalt
- VIS-Logfile Prüfung bei Migrationsamt
- Archivierung und Vernichtung bei kantonalen Stellen

14 Antrag

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

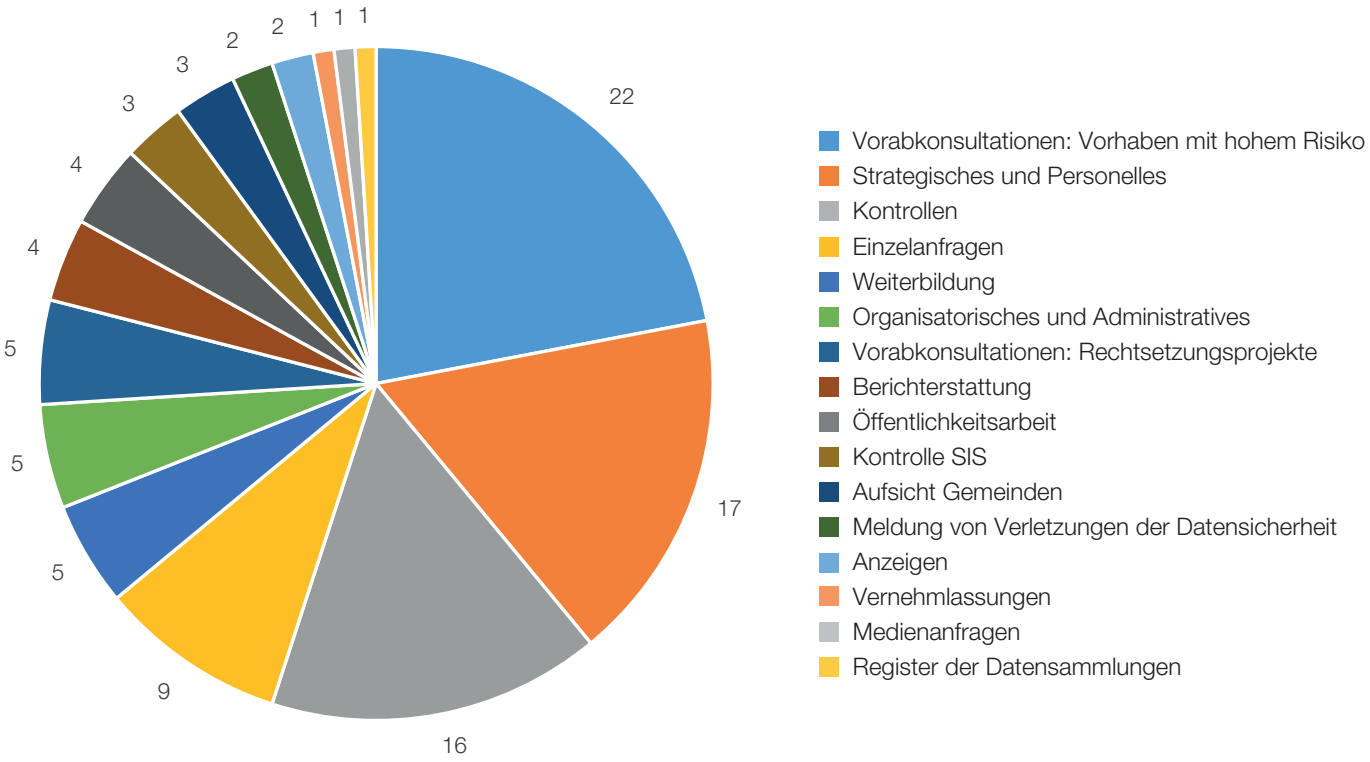
Kantonale Fachstelle für Datenschutz
Corinne Suter Hellstern, Leiterin

Geschäftseingänge[1]



1 Als Geschäftseingänge gelten Anfragen, Vorabkonsultationen, Vernehmlassungen, Anzeigen und Meldungen von Verletzungen der Datensicherheit.

Aufgabenverteilung nach Art in Prozent[2]



2 Aufgabenverteilung nach Art in Prozent gemäss interner Arbeitszeiterfassung (gerundet), 2025

Kantonsrat des Kantons St.Gallen
Geschäft 32.26.03

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