Kanton St.Gallen
Fachstelle für Datenschutz

Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2024

Inhaltsverzeichnis

Zusammenfassung

Im Berichtsjahr schloss die Fachstelle für Datenschutz (FDS) die Prüfungen PUPIL Connect und diejenige bei der St.Galler Pensionskasse (sgpk) ab. PUPIL Connect ist ein eGovernment-Projekt im Schulbereich, bei dem verschiedene Anspruchsgruppen auf mehreren Staatsebenen involviert sind. Für die Einhaltung der Datenschutzbestimmungen ist in solchen Projekten besonders wichtig, dass die Zuständigkeiten und Verantwortlichkeiten klar geregelt sind. Des Weiteren muss sichergestellt werden, dass bei allen Anspruchsgruppen datenschutzrechtliches Know-how vorhanden ist.

Die sgpk ist eine öffentlich-rechtliche Stiftung. Es musste geklärt werden, welche datenschutzrechtlichen Grundlagen anwendbar sind und wer die zuständige Aufsicht ist. Die FDS gelangte zur Auffassung, dass je nach Aufgabenbereich andere Rechtsgrundlagen anwendbar sind und entweder die FDS oder der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zuständig ist. Weil diese mehrfache Zuständigkeit auch für die öffentlichen Organe unpraktikabel ist, erklärt sich in solchen Fällen diejenige Datenschutz-Aufsicht als zuständig, in deren Zuständigkeit der grössere Teil der Aufgabenerfüllung fällt. Im Fall der sgpk ist das die FDS. Die FDS machte zudem Empfehlungen zu den Zugriffsberechtigungen auf archivierte Akten, die Webseite und die Prozesse zur Meldepflicht sowie zum Einsichtsrecht.

Die FDS prüfte aprendo, eine webbasierte Lern- und Weiterbildungsplattform für Schulleitungen und Lehrpersonen. Mit aprendo werden keine besonders schützenswerten Personendaten bearbeitet. Die FDS machte Empfehlungen zur Erstregistrierung, der Risikoeinschätzung in der Datenschutz-Folgenabschätzung und zu den Zugriffsberechtigungen.

Bei den gemeldeten Datenschutzverletzungen waren ein Ransomware-Angriff und die falsche Ablage von Dokumenten in einem Kundenportal Thema. Des Weiteren ging es um unverschlüsselte Datenträger. In einem Fall um einen Verlust, im anderen Fall um einen Diebstahl. Unverschlüsselte Datenträger bergen ein sehr hohes Risiko für eine Verletzung der Grundrechte der betroffenen Personen und sollten nicht verwendet werden. Was die Informationspflicht der betroffenen Personen anbelangt, beurteilt die FDS diese in den beiden Fällen unterschiedlich.

Bei der Aufsicht über die Gemeindefachstellen für Datenschutz waren M365 Thema sowie die vorgesehene Reorganisation. Weil der Verband St.Galler Gemeindepräsidien (VSGP) diese bis Anfang 2025 vorsah, verzichtete die FDS auf ihren Arbeitsbesuch bei der Gemeindefachstelle Rheintal Werdenberg Sarganserland. Je nachdem wird sie diesen im Jahr 2025 nachholen.

Der Kanton St.Gallen führte im Berichtsjahr M365 ein. Mit dem Swiss-U.S. Data Privacy Framework, das seit Herbst 2024 in Kraft ist, verfügen zertifizierte US-Unternehmen über ein angemessenes Datenschutzniveau. Das kann sich auf die Art der ergriffenen Massnahmen auswirken. Nichts ändert sich hingegen bezüglich des Cloud Acts. Die FDS machte verschiedene Empfehlungen, unter anderem zur Verwendung der Daten durch Microsoft.

Im Weiteren prüfte die FDS sowohl die Rechtsgrundlage als auch das Projekt zu E-Collecting. Damit sollen Unterschriften zur Unterstützung von Volksinitiativen oder Referendumsbegehren elektronisch gesammelt werden. Die FDS empfahl, Logfiles in regelmässigen Abständen mittels Stichproben manuell auf Vollständigkeit bzw. Richtigkeit zu überprüfen. Vor der Aufschaltung soll ein Pen-Test durchgeführt werden, um eventuelle Risiken zu minimieren.

Die FDS bearbeitete mehrere Anzeigen und Anfragen zur Publikationsplattform und automatisierten Text-Verarbeitung von Patientenakten.

Auf politischer Ebene wird eine engere Zusammenarbeit der Datenschutzbehörden der Kantone St.Gallen, Thurgau und beider Appenzell angestrebt. Vorgesehen ist eine Zusammenarbeit bei der Digitalisierung und bei kantonsübergreifenden Projekten. Geplant ist, dass die Vereinbarung auf Mitte 2026 in Vollzug gesetzt wird.

Frau Präsidentin
Sehr geehrte Damen und Herren

Die kantonale Fachstelle für Datenschutz (FDS) berichtet dem Kantonsrat jährlich über ihre Tätigkeit. Der Kantonsrat nimmt vom Bericht Kenntnis.[1] Der Bericht an den Kantonsrat hat dieselbe Stellung wie der Geschäftsbericht der Regierung nach Art. 5a des Staatsverwaltungsgesetzes[2].[3] Der vorliegende Bericht gibt Rechenschaft über die Tätigkeit der FDS im Jahr 2024.

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 Herausforderungen

Die Tätigkeit im Bereich Datenschutz bleibt als Ganzes herausfordernd mit der raschen Dynamik im Wechselspiel mit den technischen Entwicklungen. Dennoch sollen zu Beginn drei Punkte etwas eingehender erörtert werden, welche die FDS im Berichtsjahr mehrmals beschäftigt haben:

- Für öffentliche Organe besteht die Pflicht, Datenschutzverletzungen der FDS zu melden, wenn voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht. Zudem sind die öffentlichen Organe verpflichtet zu beurteilen, ob die betroffenen Personen informiert werden müssen. Das ist immer dann der Fall, wenn diese Vorkehrungen zu ihrem Schutz vornehmen können, wie etwa, das Passwort zu ändern. Betroffene Personen müssen unter Umständen aber auch dann informiert werden, wenn sie nicht unmittelbar eine Massnahme ergreifen können. Nur schon die Information, dass eigene Personendaten abhandengekommen sind, sensibilisiert und erhöht die Aufmerksamkeit, so dass die Person Vorgänge in ihrem Umfeld einordnen und später Massnahmen treffen kann. Das ist umso wichtiger, je sensibler die Personendaten sind. Das öffentliche Organ muss deshalb in jedem einzelnen Fall sorgfältig abwägen, ob eine Information erforderlich ist. Die öffentlichen Organe handhaben die Information sehr unterschiedlich: Einige pflegen eine transparente Kommunikation und informieren eher einmal zu viel, andere informieren auch in Grenzfällen nicht. Damit nimmt man den betroffenen Personen aber die Möglichkeit, adäquat und vorausschauend zu reagieren. Ein offener und transparenter Umgang der Verwaltung tendenziell zu Gunsten einer Information kommt letztlich nicht nur den betroffenen Personen zu Gute. Es zeichnet auch ein öffentliches Organ aus, das eine offene Fehlerkultur pflegt und sich seiner Verantwortung gegenüber den Bürgerinnen und Bürgern bewusst ist.

- Im Berichtsjahr führte der Kanton St.Gallen M365 ein (siehe dazu nachfolgend Ziff. 5.1). Seit 2024 gilt für Personendaten, die von Organisationen bearbeitet werden, die gemäss den Grundsätzen des Datenschutzrahmens zwischen der Schweiz und den USA[4] zertifiziert sind, ein angemessenes Schutzniveau als gewährleistet. Microsoft als Anbieterin von M365 ist ein zertifiziertes Unternehmen gemäss diesem Datenschutzrahmen. Für öffentliche Organe bedeutet das, dass wenn sie bei einem zertifizierten US-Unternehmen Personendaten bearbeiten lassen eine vergleichbare Ausgangslage besteht, wie bei den übrigen Staaten, welche in der Verordnung des Bundesrates als Staaten mit angemessenem Datenschutz gelten. Dazu zählen die Staaten der EU. Das kann Auswirkungen bei den zu ergreifenden Sicherheitsmassnahmen haben. Keine Änderung gibt es hingegen bezüglich des Cloud Acts. Dieser ermöglicht staatlichen Stellen ohne Weg über die internationale Rechtshilfe auf in- und ausländische Server Zugriff zu nehmen. Damit besteht die Gefahr einer Offenbarung etwa des Berufsgeheimnisses ohne Rechtfertigungsgrund. Die FDS hat in ihren Tätigkeitsberichten darauf hingewiesen.[5] Dabei handelt es sich nicht um ein Risiko, sondern um eine rechtliche Schranke. Diese kann nicht mit technischen oder organisatorischen Massnahmen beseitigt werden. Nach wie vor dürfen deshalb keine Personendaten in M365 bearbeitet werden, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen. In diesem Fall ist eine Bearbeitung nach wie vor nur zulässig, wenn die Personendaten verschlüsselt werden und das Schlüsselmanagement beim öffentlichen Organ liegt.

- Die FDS stellt vor allem bei Vorhaben mit hohem Risiko immer wieder fest, dass öffentliche Organe zwar die IT-Sicherheit abklärten und diese Unterlagen vorliegen. Die rechtlichen Abklärungen hingegen fehlen teilweise oder vollständig. Häufig sind keine Rechtsgrundlagenanalysen vorhanden. Auch die Auseinandersetzung mit der Verhältnismässigkeit findet oft nicht statt. Der erste Schritt zur Abklärung, ob eine bestimmte Datenbearbeitung zulässig ist, führt über das Recht. Aufgrund des Legalitätsprinzips ist sämtliches staatliches Handeln an das Recht gebunden. Erst wenn eine genügende Rechtsgrundlage vorhanden ist, kann überhaupt geprüft werden, welche Massnahmen technischer und organisatorischer Art ergriffen werden müssen, um die Datenschutzbestimmungen einzuhalten. Aus Sicht der FDS muss sichergestellt werden, dass bei jedem Vorhaben, das die Bearbeitung von Personendaten betrifft, vorab die rechtlichen Aspekte geprüft werden und entsprechendes Wissen in den Projektorganisationen vorhanden ist.

4
Swiss - U.S. Data Privacy Framework.

5
Siehe Tätigkeitsberichte der Fachstelle für Datenschutz über das Jahr 2022, S. 15 und 2023, S. 17.

2.1 PUPIL Connect

Im Berichtsjahr schloss die FDS die Prüfung zu PUPIL Connect (vormals PUPIL messenger) ab. Dabei handelt es sich um einen Messenger, der den Volksschulträgern für die Kommunikation mit den Eltern dient. Er kann als App oder als Webapplikation verwendet werden. PUPIL Connect ist Teil des Projekts PUPIL, eine Schulmanagementsoftware der Schulträger und des Amtes für Volksschule. Es handelt sich um ein eGovernment-Projekt. Die datenschutzrechtliche Aufsicht über die Volksschulträger liegt bei den Gemeindefachstellen für Datenschutz, daher wurden auch diese in die Prüfung einbezogen.

Bei E-Government-Projekten sind viele Anspruchsgruppen auf verschiedenen Staatsebenen mit unterschiedlichen Bedürfnissen involviert. Das macht diese Vorhaben sehr komplex. Kommt hinzu, dass im Schulbereich viele und häufig sensible Personendaten bearbeitet werden. Sehr wichtig ist deshalb, dass die Zuständigkeiten und Verantwortlichkeiten klar geregelt und kommuniziert werden. Für die Einhaltung der Datenschutzbestimmungen ist das eine unabdingbare Voraussetzung.

Zur Rechtsgrundlage äusserte sich die FDS bereits im Rahmen der Vorabkonsultation von PUPIL[6]. Die FDS vertritt die Auffassung, dass die Bearbeitung von Personendaten im Schulbereich generell in den Grundzügen in einem formellen Gesetz geregelt werden muss.

Es ist wichtig, dass klar definiert ist, für welche Zwecke PUPIL Connect verwendet wird. Dabei muss der Zweck eng – auf die nicht heikle Kommunikation zwischen Lehrpersonen und Erziehungsberechtigten – ausgelegt werden. Für sensible Datenbearbeitungen ist die Schulverwaltungssoftware PUPIL gedacht. Der Charakter eines Messengers birgt mehr Problematiken seitens der End-Nutzenden, die sich allenfalls nicht überlegen, ob eine Mitteilung heikel sein könnte. Die Anwendung wird zudem mit «vertraulich» klassifiziert. Somit dürfen keine besonders schützenswerten Personendaten in PUPIL Connect bearbeitet werden. Problematisch in diesem Zusammenhang ist die Verwendung von Freitextfeldern. Sie lassen grossen Spielraum für heikle Datenbearbeitungen zu.

Die Bearbeitungsregeln müssen allen anwendenden Personen bekannt sein. Ein klar eingegrenzter Einsatz von PUPIL Connect und eine gute Information und Sensibilisierung derjenigen, welche PUPIL Connect anwenden, trägt dazu bei, dass die Datenschutzbestimmungen eingehalten werden können.

Ein besonderes Augenmerk muss auf die Verwendung des Übersetzungstools gelegt werden. Dabei kann nicht ausgeschlossen werden, dass diese Daten in einem Land mit einem nicht angemessenen Datenschutzniveau bearbeitet werden, insbesondere in den USA. Sensible Datenbearbeitungen sind damit nicht zulässig und es sollten entsprechende Weisungen bestehen.

Zwar kennt das DSG keine Pflicht, Datenschutzberaterinnen und -berater zu ernennen. Allerdings sind die datenbearbeitenden Stellen für die Einhaltung des Datenschutzes verantwortlich. Diese Verantwortung des öffentlichen Organs bleibt auch im Fall einer Auftragsdatenbearbeitung bestehen. Die Verantwortung kann angesichts der Komplexität der Thematik nur angemessen wahrgenommen werden, wenn Grundkenntnisse

6 Siehe Tätigkeitsbericht der Fachstelle für Datenschutz über das Jahr 2022, S. 13.

des Datenschutzes und der IT-Sicherheit vorhanden sind. Sowohl die Vertragspartnerin eGovernment St.Gallen digital. als auch die Leistungsbezüger (Volksschulen) sollten über datenschutzberatende Stellen verfügen.

Ein klar definierter und funktionierender Prozess bei einer Verletzung der Datensicherheit ist wichtig. Einen solchen haben die Verantwortlichen beim Bildungsdepartement erstellt. Allerdings kann eine Verletzung auch einen Schulträger betreffen. Auch dort muss klar definiert werden, wer in einem solchen Fall was wann tun muss. Dasselbe gilt für eGovernment St.Gallen digital.

Des Weiteren machte die FDS Empfehlungen zum Auftragsdatenbearbeitungsvertrag, zu den Aufbewahrungsfristen und zur Löschung der Daten. Im Produktivsystem sollten zudem keine unpersönlichen Accounts verwendet werden.

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

2.2 St.Galler Pensionskasse

Die FDS prüfte Datenschutz und IT-Sicherheit bei der St.Galler Pensionskasse (sgpk). Vorerst war zu klären, ob auf die öffentlich-rechtliche Stiftung eidgenössisches oder kantonales Datenschutzrecht anwendbar und wer datenschutzrechtliche Aufsicht ist. Die FDS gelangte zur Auffassung, dass je nach Rechtsverhältnis und Aufgabenbereich für die sgpk das eidgenössische oder das kantonale Datenschutzgesetz anwendbar ist. Bei der Frage der Aufsicht ist davon auszugehen, dass der überwiegende Teil der Aufgabenerfüllung der sgpk unter die Aufsicht der FDS fällt. Die FDS orientiert sich am informellen Beschluss von privatim (Konferenz der schweizerischen Datenschutzbeauftragten), wonach bei überwiegend hoheitlichem Handeln durch kantonale Behörden die Kantone die Aufsicht ausüben sollen. Diese Regelung ist im Sinn der öffentlichen Organe, müssen sie doch nicht jeweils im einzelnen Fall erst eruieren, wer nun zuständige Datenschutz-Aufsichtsstelle ist. Die FDS erachtet es deshalb als vertretbar, dass die FDS, unabhängig von der wahrgenommenen Aufgabe, dem Anschluss und der anwendbaren Rechtsgrundlage, zuständige Datenschutz-Aufsicht ist.

Die sgpk digitalisierte das Archiv der Versichertenverwaltung. Abgesehen von zwei Ausnahmen werden alle Dokumente nur noch elektronisch archiviert. Die Unterlagen werden im Kundendienst aufbewahrt. Zugriff haben alle Mitarbeitenden. Die FDS empfahl, die Zugriffe einzuschränken. Auch bei archivierten Akten dürfen nur diejenigen Personen Zugriff haben, welche sie für ihre gesetzliche Aufgabenerfüllung benötigen.

Die Webseite der sgpk verwendet Cookies. Der Cookie-Banner erschien beim ersten Aufruf der Webseite, danach nicht mehr. Tools, welche das Nutzerverhalten auswerten, dürfen öffentliche Organe nicht einsetzen. Sie müssen sicherstellen, dass keine solchen Tools eingesetzt werden. Die Webseiten-Besuchenden müssen die Möglichkeit haben, Cookies abzulehnen. Eine entsprechende Meldung muss bei jedem Aufruf der Webseite platziert werden. Google Analytics sollte nicht verwendet werden. Auf Anfang 2025 hat die sgpk Google Analytics durch ein anonymes Tool ersetzt.

Es fehlten sowohl im Fall von Einsichtsgesuchen von Betroffenen als auch im Fall einer Verletzung der Datensicherheit Prozesse. Es ist wichtig, diese im Vorfeld zu definieren und die Verantwortlichkeiten klar zu regeln. Gerade in Fällen von Verletzungen der Datensicherheit, in denen die vom Datenschutz-Vorfall betroffenen Personen informiert werden müssen, muss rasch gehandelt werden.

Die zentrale Bereitstellung der Informatik hat die sgpk an den Dienst für Informatikplanung (DIP) ausgelagert. Während des Zeitpunktes der Prüfung fanden in diesem Bereich Änderungen statt. Eine entsprechende Dokumentation lag damals nicht vor und wurde auch nach mehrmaliger Aufforderung nicht nachgereicht. Ohne Dokumentation ist eine Prüfung nicht möglich. Die Prüfung umfasste diesen Teil deshalb nicht. Die FDS verwies die sgpk darauf, dass sie als datenbearbeitendes Organ verantwortlich ist und sicherstellen muss, dass auch dieser Bereich datenschutzkonform betrieben wird.

Die sgpk hat die Empfehlungen angenommen und mehrheitlich bereits umgesetzt.

2.3 Weiterbildungsplattform aprendo

Im Jahr 2024 prüfte die FDS die Weiterbildungsplattform aprendo der Pädagogischen Hochschule St.Gallen (PHSG). Aprendo ist eine webbasierte Lern- und Weiterbildungsplattform für Schulleitungen und Lehrpersonen. Die PHSG entwickelte sie im Rahmen der IT-Bildungsoffensive. Damit sollen die digitalen und mediendidaktischen Kompetenzen unterstützt und der Einsatz von digitalen Medien in der Schule und im eigenen Unterricht sinnvoll ermöglicht werden.

Mit aprendo werden keine besonders schützenswerten Personendaten, Persönlichkeitsprofile oder Profilings bearbeitet. Zwar werden die Daten zu besuchten und abgeschlossenen bzw. abgebrochenen Kursen so lange aufbewahrt, wie die Kursteilnehmenden aprendo nutzen. Das kann je nach Fall eine lange Zeitdauer sein. Weil die Kurse aber ausschliesslich im Bereich neue Medien / Medienpädagogik / Informatik angeboten werden, qualifiziert die FDS diese Daten auch bei einer längeren Aufbewahrung (Längsschnitt) nicht als ein Persönlichkeitsprofil.

Innerhalb von aprendo werden zwei Dienste aus einem Land mit einem nicht angemessenen Datenschutzniveau verwendet. Es handelt sich um eine Auftragsdatenbearbeitung. Das Risiko des Einsatzes dieser beiden Dienste wurde im Rahmen einer Datenschutz-Folgenabschätzung[7] eruiert und Massnahmen dargelegt. Der FDS fehlte in diesem Zusammenhang aber die Auseinandersetzung mit dem Risiko, dass Modul-Leitende und Lehrpersonen in Wort und Bild aufgenommen werden. Angesichts der Entwicklungen im Bereich der KI mit grossen auch wirtschaftlichen Interessen an allen Arten von Daten kann das ein hohes Risiko darstellen. Die FDS empfahl deshalb, dieses Risiko auszuweisen, zu bewerten und Massnahmen aufzuzeigen.

Die Einwilligung zur Erstregistrierung für Lehrpersonen und Schulleitungen empfahl die FDS zu präzisieren. Aufgrund des vorliegenden Dokuments und der Formulierung war zu wenig klar, dass Lehrpersonen und Schulleitungen damit eine Einwilligung zur Datenbearbeitung erteilen.

7 Art. 8a DSG.

Ein weiteres Thema waren die Zugriffsberechtigungen. Die FDS empfahl, den Zugang zur Weiterbildungsplattform auf Lehrpersonen und Schulleitungen einzuschränken. Auch die Zugriffe auf die Backup-Systeme sollten eingeschränkt werden, ebenso der Zugriff auf die Schlüssel für die Verschlüsselung. Darauf darf nur ein eng begrenzter Kreis Zugriff haben, der die Schlüssel für die Aufgabenerfüllung benötigt. Es ist nicht ersichtlich, wozu Mitglieder der Geschäftsleitung einen solchen Schlüssel benötigen. Des Weiteren muss aprendo im Register der Datensammlungen[8] aufgeführt werden.

8
Register der Datensammlungen | sg.ch

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

2.4 CONNET

Die FDS führte die Prüfung der Heimverwaltungslösung CONNET beim Amt für Soziales Ende des Berichtsjahres durch. Sie ist noch nicht abgeschlossen.

2.5 Schengen-Kontrolle bei der Kantonspolizei

Die FDS sah im Berichtsjahr eine Schengen-Kontrolle bei der Kantonspolizei vor. 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. Periodisch soll die Rechtmässigkeit der Bearbeitung personenbezogener Daten im SIS kontrolliert werden; das gilt ebenso für das VISA-Informationssystem. In diesem Bereich hat die FDS bisher keine Prüfung durchgeführt, weshalb sie eine VISA-Prüfung bei der Kantonspolizei vorsah. Nach längeren Recherchen stellte sich heraus, dass die Mitarbeitenden der Kantonspolizei keinen Zugriff auf das VISA-Informationssystem haben. Somit erübrigt sich auch eine Logfile-Kontrolle. Die FDS wird nun für das Jahr 2025 eine Logfile-Kontrolle des SIS bei der Kantonspolizei vorsehen.

2.6 Zugriffe auf kantonale Einwohnerdatenplattform

In den Vorjahren hat die FDS bereits bei mehreren Stellen in verschiedenen Departementen die Zugriffe auf die kantonale Einwohnerdatenplattform (KEWR) geprüft. Für das Berichtsjahr sah sie deshalb eine Prüfung der Datenbank KEWR vor. Die zuständige Stelle informierte daraufhin, dass die Plattform per Mitte 2025 durch das Personenregister abgelöst werde. Die FDS sah deshalb von der Prüfung ab und wird im Jahr 2026 das Personenregister prüfen. Die heute im KEWR enthaltenen Daten werden erweitert durch Personendaten aus dem Migrationsbereich und Personen, die in einem steuerrechtlichen Verhältnis zum Kanton St.Gallen stehen. Somit werden im Personenregister die Stammdaten sämtlicher Personen bearbeitet, die einen Bezug zum Kanton St.Gallen haben. Dieses Vorhaben hätte der FDS zur Vorabkonsultation vorgelegt werden müssen. Das war nicht der Fall. Weil sich das Projekt bereits in der Realisierungsphase befand, wird die FDS das Personenregister nach der Einführung prüfen.

3 Meldungen Verletzung Datensicherheit

3.1 Verlust unverschlüsselter USB-Stick

Ein öffentliches Organ bearbeitete ein Auskunfts- und Einsichtsgesuch eines Arbeitnehmers. Es schickte dessen Rechtsvertreter mit A-Post Plus ein digitales Personaldossier zusammen mit aktualisierten digitalen Verfahrensakten, die auf einem unverschlüsselten USB-Stick gespeichert waren, zu. Bei der Rücksendung ging der USB-Stick «durch ein Missgeschick der Post» verloren. Auf dem USB-Stick befanden sich besonders schützenswerte Personendaten verschiedener Personengruppen. Die Anzahl der betroffenen Personen wurde auf 15 bis 40 geschätzt.

Unverschlüsselte Sticks bergen ein sehr hohes Risiko für Datenschutzverletzungen und sind für solch sensible Daten, wie sie vorliegend bearbeitet wurden, nicht geeignet. Es dürfen – sofern der Einsatz von USB-Sticks unumgänglich ist – nur noch USB-Sticks verwendet werden, deren Inhalt verschlüsselt ist. Taucht der USB-Stick auf, muss das öffentliche Organ prüfen, ob ein Zugriff auf den USB-Stick stattgefunden hat. Besteht die Gewissheit oder eine sehr grosse Wahrscheinlichkeit, dass kein Zugriff auf den USB-Stick stattgefunden hat, ist eine Information an die betroffenen (Dritt-)Personen nicht erforderlich. Andernfalls sollen die betroffenen Personen über den Vorfall informiert werden. Zudem soll die Sensibilisierung weiter optimiert werden und regelmässig erfolgen. Der Vorfall muss dokumentiert und die Unterlagen dazu müssen aufbewahrt werden. Dies dient der Beweispflicht, wonach das öffentliche Organ für die Einhaltung der Datenschutzbestimmungen beweispflichtig ist.

3.2 Diebstahl unverschlüsselter Datenträger

Ein weiterer Vorfall betraf den Diebstahl eines unverschlüsselten Datenträgers. Aus dem Auto von Mitarbeitenden einer privaten Institution wurde eine Festplatte gestohlen. Das öffentliche Organ hat sich bei dieser privaten Institution zwecks eigener gesetzlicher Aufgabenerfüllung eingemietet. Es werden gemeinsame Datenträger verwendet. Die Festplatte wird für Backups genutzt, üblicherweise von einer Mitarbeiterin oder einem Mitarbeiter mit nach Hause genommen und in der Wohnung aufbewahrt. Es befanden sich u.a. besonders schützenswerte Personendaten von Mitarbeitenden sowie Klientinnen und Klienten des öffentlichen Organs darauf.

Auch wenn die Festplatte aus dem Auto eines Mitarbeitenden der privaten Institution gestohlen wurde, bleibt das öffentliche Organ verantwortlich, wenn Personendaten seiner Klientinnen und Klienten betroffen sind. Die Einhaltung des Datenschutzes muss in einer Vereinbarung geregelt und kontrolliert werden. Die FDS ist der Ansicht, dass das Risiko für die betroffenen Personen bei einem Diebstahl i.d.R. höher ist als bei einem Verlust etwa durch Liegenlassen. Bei einem Diebstahl ist bereits eine kriminelle Absicht vorhanden, die sich auf die gestohlenen Daten auswirken kann. Dies beeinflusst die Beurteilung, ob die betroffenen Personen informiert werden müssen, was die FDS in diesem Fall bejahte. Im Übrigen sollten Festplatten nicht nach Hause genommen und dort aufbewahrt werden. Unverschlüsselte Datenträger sind zudem für besonders schützenswerte Personendaten nicht zulässig. Schliesslich sollte die Sensibilisierung aller Mitarbeitenden weiter optimiert werden und regelmässig erfolgen.

3.3 Falsche Ablage in Kundenportal

Weitere Fälle betrafen falsche Ablagen in einem Kundenportal. Ein Dokument mit besonders schützenswerten Personendaten wurde beim Einscannen mit dem falschen Fall verknüpft und dadurch einer anderen Person zugewiesen. Die FDS empfahl, bei der Zuweisung eines Dokumentes vor der endgültigen Zuweisung eine Systemmeldung zu generieren, welche die Mitarbeitenden fragt, ob das entsprechende Dokument definitiv in das Dossier der angewählten Person verschoben werden soll. Zudem muss auch bei solchen Meldungen, die Vorfälle betreffen, welche häufiger vorkommen, das Risiko für die betroffene Person beschrieben und mitgeteilt werden, ob die betroffene Person über den Vorfall informiert wurde oder mit welcher Begründung nicht.

3.4 Ransomware-Angriff

Nach einem Ransomware-Angriff auf eine Institution im Schulbereich wurden Daten von Lehrpersonen und Lernenden verschlüsselt. Nebst Kontaktdaten waren auch Standortbestimmungen betroffen. Ransomware-Angriffe zielen typischerweise darauf ab, Daten zu verschlüsseln und nicht darauf, Daten einzusehen. Die Angreifer waren nur kurze Zeit im System. Das öffentliche Organ erachtete es als unwahrscheinlich, dass die Angreifer in dieser Zeit nebst der Verschlüsselung auch noch Einsicht in Personendaten nehmen konnten. Aufgrund der hohen Komplexität des Systems wäre eine Einsicht mit einem grossen Aufwand verbunden gewesen. In dieser Zeit sei es zudem unmöglich gewesen, eine Datenbank unbemerkt aus dem Rechenzentrum zu kopieren. Das öffentliche Organ stufte deshalb das Risiko für die betroffenen Personen nicht als hoch ein und verzichtete auf eine Information. Aufgrund ihrer Prüfung erachtete die FDS die Argumentation als plausibel und teilte die Einschätzung des öffentlichen Organs. Sie empfahl künftig auf die Erhebung des Geburtsdatums als Personenidentifikator zu verzichten. Ebenfalls wurde empfohlen ein Löschkonzept zu erstellen und einen Prozess zur Meldung von Verletzungen der Datensicherheit zu definieren. Zudem sollen die Mitarbeitenden für die Problematik von Datenschutzverletzungen sensibilisiert und geschult werden.

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, die Stadt St.Gallen hat eine eigene Stelle. Der Verband St.Galler Gemeindepräsidien (VSGP), als Trägerverein der politischen Gemeinden, beabsichtigt, die heutige Organisation zu ändern. Es ist nicht nur rechtliches, sondern auch Know-how im Bereich der Informationssicherheit vorgesehen. Der VSGP hat die FDS über das Vorhaben informiert. Als Aufsichtsorgan über die Gemeindefachstellen für Datenschutz hat sich die FDS zu den Leitplanken geäussert: Die Organisation muss in ihrer Aufgabenerfüllung unabhängig sein und über genügend Ressourcen für ihre gesetzlichen Aufgaben verfügen. Die FDS schätzt, dass diese etwa 200 bis 250 Stellenprozente betragen sollten. Diese Schätzung umfasst auch Know-how im IT-Bereich und die Stellvertretung.[9]

4.2 Arbeitsbesuch

Im Berichtsjahr sah die FDS einen Arbeitsbesuch bei der Fachstelle für Datenschutz Rheintal Werdenberg Sarganserland vor. Wie in Ziff. 4.1 erwähnt, plant der VSGP eine Reorganisation der heutigen Organisation der Gemeindefachstellen. Ursprünglich war diese auf Anfang 2025 vorgesehen. Die FDS verzichtete deshalb auf den Arbeitsbesuch bei der Gemeindefachstelle Rheintal Werdenberg Sarganserland, der im November 2024 geplant war. Je nachdem, wie und wie rasch das Vorhaben umgesetzt wird, wird die FDS den Arbeitsbesuch nachholen.

4.3 M365 bei den Gemeinden

Auch bei den Gemeinden ist M365 Thema. Damit die Gemeinden dies einheitlich handhaben können, erarbeitete die für die digitale Transformation zuständige Stelle des Kantons einen Leitfaden für die Grundkonfigurationen. Die FDS prüfte diese Grundkonfigurationen aus technischer Sicht. Der Leitfaden zeigt den Gemeinden auf, mit welchen Voreinstellungen die jeweiligen Produkte von Microsoft bestellt werden müssen, damit sie datenschutzkonform sind.

4.4 Erfahrungsaustausch

Am regelmässigen Austausch der FDS mit den Gemeindefachstellen für Datenschutz waren M365 bei den Gemeinden Thema, ebenso die Prüfung von PUPIL Connect und erste Erfahrungen der Schulgemeinden mit PUPIL. Des Weiteren die vorgängige Konsultation bei Merkblättern und Checklisten der FDS und der U.S. Data Privacy Framework.

9

Die Schätzung stützt sich auf einen Aufsatz von Beat Rudin (Beat Rudin, die datenschutzrechtliche Umsetzung von Schengen in den Kantonen, in: Breitenmoser / Gless / Lagodny (Hrsg.), Schengen in der Praxis, Dike Verlag, 2009, S. 213 ff.). Er hat Kriterien aufgestellt, nach denen sich die erforderlichen Stellenprozente bemessen lassen können. Zu berücksichtigen ist, dass der Aufsatz über 15 Jahre alt ist und der Datenschutz insbesondere auch mit der Digitalisierung und dem damit erforderlichen technischen Know-how stark an Bedeutung gewonnen hat. Deshalb rechtfertigt sich ein Zuschlag zu den dargelegten Zahlen.

5 Vorhaben mit hohem Risiko

5.1 M365

Der Kanton St.Gallen führte M365 rollend ab Herbst 2024 ein. Entgegen der ersten Absicht können nun auch Personendaten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen in der Cloud von Microsoft bearbeitet werden. Wie einführend bereits erwähnt (siehe Ziff. 1), widerspricht dieser Punkt nach Ansicht der FDS datenschutzrechtlichen Vorgaben und die Regierung muss die politische Verantwortung für diesen Umstand übernehmen.

Der Kanton entschied, dass Fachapplikationen weiterhin bestehen bleiben. Es ist sehr wichtig, dass dies auch langfristig der Fall ist. In Fachapplikationen werden häufig die besonders sensiblen Daten bearbeitet. Diese dürfen nicht in der Cloud bei einem Anbieter in einem Land mit nicht angemessenem Datenschutzniveau und Cloud Act gehostet werden.

Mit der Einführung von M365 sind die Mitarbeitenden verpflichtet, die Dokumente je nach Sensibilität selbst zu klassifizieren (Labeling). Dabei besteht das Risiko, dass Dokumente falsch klassifiziert werden. Die FDS empfahl deshalb zu prüfen, standardmässig sämtliche kritischen Dokumente mit «geheim» zu klassifizieren.

Die FDS hat im Weiteren Folgendes empfohlen:

- Es muss vertraglich sichergestellt werden, dass Microsoft die bearbeiteten Personendaten gemäss dem Grundsatz der Zweckmässigkeit nur für die vereinbarten Zwecke (Hilfsmittel zur Erfüllung der gesetzlichen Aufgaben des Kantons) verwenden darf. Angesichts der Herausforderungen von künstlicher Intelligenz (KI) ist das umso dringlicher: Für das Training von KI braucht es sehr viele Daten. Eine Verwendung der Daten für dieses Training ist nicht zulässig. Zudem kann nicht ausgeschlossen werden, dass die aus der KI entstehenden Produkte Rückschlüsse auf Personen ermöglichen. Es muss deshalb sichergestellt werden, dass die Personendaten nicht für das Training von KI verwendet werden.

- Es muss eine Exit-Strategie vorhanden sein. Dies, weil im Fall einer Vertragsverletzung oder anderer Verstösse gegen Datenschutzvorschriften das öffentliche Organ gesetzlich verpflichtet ist, die Übertragung rückgängig zu machen.[10] Das öffentliche Organ muss deshalb regelmässig Alternativen prüfen und einen allfälligen Wechsel evaluieren. Das ist auch angezeigt, um die grosse Abhängigkeit von Microsoft zu reduzieren.

- Wenn Daten von Bürgerinnen und Bürger in der Cloud von Microsoft bearbeitet werden, muss dies transparent ausgewiesen werden. Die Einhaltung der Datenschutzbestimmungen ist eine wichtige Voraussetzung für das Vertrauen der Bevölkerung in die Digitalisierung durch öffentliche Organe.

10 Art. 9 Abs. 3 DSG.

5.2 Tutoris

Tutoris ist eine Fachanwendung im Migrationswesen. Die Verantwortung für das System liegt beim Trägerverein Integrationsprojekte St.Gallen (TISG) der Gemeinden. Derzeit können TISG und die Gemeinden bereits elektronisch Daten und Dokumente austauschen. Geplant ist eine zusätzliche Schnittstelle zwischen dem Migrationsamt des Kantons und der TISG. Damit sollen durchgängig digitale Prozesse ermöglicht werden.

Die FDS machte verschiedene technische Empfehlungen, so zur Wiederherstellung von Backups, zur Verschlüsselung und zum Logging. Sie stellte zudem fest, dass die Zugriffsberechtigungen auf Tutoris zu weit sind. Es dürfen nur Personen Zugriff haben, welche die Daten für ihre gesetzliche Aufgabenerfüllung benötigen. Weil diese Feststellung Organe der Gemeinden betrifft, sind die Gemeindefachstellen für Datenschutz zuständige Datenschutz-Aufsicht. Die FDS hat ihre Feststellung deshalb an sie weitergeleitet.

5.3 SAP HCM

Die Personaladministrationssoftware SAP sollte abgelöst werden. Die Schnittstellenintegration sollte neu über die SAP Integration Suite in der Cloud in Schweizer Rechenzentren erfolgen. Die FDS machte Empfehlungen zur Verhältnismässigkeit, Zweckbestimmung, Protokollierung/Logfiles, Informationspflicht, Berechtigungen/Zugriffe, Penetration Tests und Sensibilisierung. Der Vertrag mit Dritten soll datenschutzkonform ausgestaltet werden. Die Weiterübertragung der Datenbearbeitung bedarf der vorgängigen schriftlichen Zustimmung des öffentlichen Organs. Subunternehmer aus einem Land mit nicht angemessenem Datenschutzniveau müssen ausgeschlossen werden. Personendaten, die einer besonderen Geheimhaltung unterstehen, können nur dann in die Cloud von Anbietern, die dem CLOUD Act unterstehen, ausgelagert werden, wenn durch eine technische Massnahme das Offenbaren dieser Personendaten ausgeschlossen werden kann. Des Weiteren ist die FDS der Ansicht, dass eine pauschale Aufbewahrungsdauer von zehn Jahren nicht angemessen ist.

5.4 Electronic Monitoring

Electronic Monitoring (EM) ist der elektronisch überwachte Vollzug einer Freiheitsstrafe ausserhalb der Vollzugseinrichtung. Dabei wird eine Person mit einem Sender überwacht, damit ihre Anwesenheits- bzw. Positionsdaten erfasst und aufgezeichnet werden können. Das geschieht i.d.R. mit einer elektronischen Fussfessel oder einem elektronischen Armband.
Die FDS nahm sowohl zum Projekt als auch zur Rechtsgrundlage (siehe nachfolgend Ziff. 6.1) Stellung. EM ist im Kanton St.Gallen bereits seit dem Jahr 2018 im Einsatz. Nun wird die technische Lösung erneuert und es soll die schweizweite Lösung des Vereins Electronic Monitoring eingeführt werden. Vorgesehen ist neu ein Alkoholmonitoring, d.h., eine kontinuierliche oder zeitweise Alkoholkontrolle. Feldgeräte würden von der Aktivierung bis zur Deaktivierung der Überwachung Blutalkoholkonzentrationswerte sammeln. Ferner ist geplant, dass das Opfer Electronic Monitoring verwenden kann, sofern einverstanden. Zudem soll für eine höhere Auflösung Google Maps verwendet werden.

Für die Überwachung des Alkoholkonsums gibt es keine formell-gesetzliche Grundlage. Sie ist deshalb nicht zulässig, ausser gestützt auf einen Entscheid durch ein Gericht im Einzelfall. Dasselbe gilt für die Überwachung des Opfers. Für öffentliche Organe gilt grundsätzlich das Legalitätsprinzip, d.h. jede Datenbearbeitung erfordert eine Rechtsgrundlage. Eine Einwilligung ist nur im Einzelfall und subsidiär zulässig. Eine systematische Datenbearbeitung kann deshalb nicht auf Einwilligungen gestützt werden.

Sofern der Einsatz von Google Maps lediglich einer höheren Auflösung dient, ist die Verwendung nicht erforderlich und deshalb nicht datenschutzkonform.

5.5 E-Collecting

Mit E-Collecting sollen elektronische Unterschriften zur Unterstützung von Volksinitiativen oder Referendumsbegehren – entweder anstelle von Unterschriften auf Papier oder in Kombination mit diesen – gesammelt werden. Die Bürgerinnen und Bürger loggen sich für den Zugriff auf das Portal einmal ein und werden auf diese Weise eindeutig authentifiziert.

Die FDS empfahl, Logfiles in regelmässigen Abständen mittels Stichproben manuell auf Vollständigkeit bzw. Richtigkeit zu überprüfen. Vor der Aufschaltung soll ein Pen-Test[11] durchgeführt werden, um eventuelle Risiken zu minimieren. Mittels Sensibilisierung und Weiterbildung soll zudem sichergestellt werden, dass alle Anwendenden die Rechtsgrundlagen und Voraussetzungen für Datenbekanntgaben kennen. Da die Prüfung durch die FDS in einem frühen Zeitpunkt stattfand und der Auftragsdatenbearbeitungsvertrag noch nicht vorlag, verwies die FDS auf die Wichtigkeit, diesen datenschutzkonform auszugestalten.

11
Ein Penetrationstest ist ein umfassender Sicherheitstest einzelner Rechner, Netzwerke oder Anwendungen. Er prüft die Sicherheit von Systembestandteilen und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die tauglich sind, um unautorisiert in das System einzudringen (Quelle: Wikipedia, Stand: Februar 2025).

5.6 E-Login

E-Login ist ein E-Government-Basisservice. Damit soll Bürgerinnen und Bürgern eine einheitliche Authentifizierungslösung für die Nutzung sämtlicher E-Government-Services bereitgestellt werden. Die FDS machte Empfehlungen zur Sensibilisierung und Weiterbildung sowie zur technischen Umsetzung. Die FDS verwies zudem darauf, dass es wichtig sei, die Auftragsdatenbearbeitungsverträge datenschutzkonform auszugestalten.

6 Rechtsetzung

6.1 Verordnung über die elektronische Überwachung

Zur Verbesserung des Schutzes gewaltbetroffener Personen wurde EM ab 1. Januar 2022 auf Bundesebene eingeführt. Die Regelung wird auf kantonaler Ebene in der Verordnung über die elektronische Überwachung umgesetzt. Die FDS empfahl, dass die Personendaten in jedem Fall verschlüsselt weitergeleitet werden müssen. Die bearbeiteten Personendaten müssen zudem samt Backups unverzüglich nach Abschluss der Massnahme vernichtet werden, falls sie die Strafverfolgungsbehörde nicht benötigt. Es soll nicht parallel zum Dossier bei der Strafverfolgungsbehörde ein weiteres Dossier geführt werden.

6.2 Nutzungsrichtlinie M365

Die Nutzung von M365[12] wird in einer Richtlinie geregelt, je für die zentrale Verwaltung und die Bildungseinrichtungen. Dazu nahm die FDS Stellung. Bei der Richtlinie für die zentrale Verwaltung machte die FDS Empfehlungen zu den Gastkonten und zur Erstellung eines Teams-Raums. In ihrer Stellungnahme zur Nutzungsrichtlinie der Bildungseinrichtungen verwies die FDS darauf, dass M365 lediglich eine temporäre Datenablage sein dürfe. Danach müssen die Personendaten in M365 unwiderruflich vernichtet werden. Zudem müssen alle Personendaten klassifiziert werden. Das ist eine wichtige Voraussetzung für das Labeling durch die Mitarbeitenden.

12 Siehe dazu auch Ziff. 5.1.

6.3 IX. Nachtrag über Referendum und Initiative

Mit der Vorlage soll E-Collecting eingeführt und die Grundlage für das E-Login geschaffen werden. Die FDS machte Empfehlungen zur Richtigkeit von Personendaten und zur Zweckbestimmung: Bei der Umsetzung soll ein besonderes Augenmerk darauf gerichtet werden, dass die Unterlagen, soweit sie in Papierform und elektronisch eingereicht werden, nur der betreffenden Person zugeordnet werden. Damit wird dem Grundsatz der Richtigkeit der Personendaten entsprochen. Im Zusammenhang mit Datenbekanntgabe an ein E-Government-Portal müssen die dafür erfassten Personendaten den gleichen Zweck verfolgen oder aber eine Rechtsgrundlage erlaubt die Bearbeitung für andere Zwecke.

Da E-Collecting auch für die kommunalen direktdemokratischen Instrumente in den politischen Gemeinden genutzt werden soll, hat die FDS die Gemeindefachstellen für Datenschutz in ihre Vernehmlassungsantwort einbezogen.

6.4 Verordnung über die polizeilichen Datenverarbeitungssysteme

Die Verordnung legt fest, welche Daten durch die Polizei gespeichert und wie lange sie aufbewahrt werden dürfen. Die FDS bemängelte den sehr umfassenden Katalog von Personalien, die gespeichert werden können. Die Regelungen sind teilweise zu offen und nicht abschliessend formuliert. Aus Sicht der Rechtssicherheit sollte die Aufzählung von Personendaten, die gespeichert werden können, abschliessend formuliert werden. Bei Datenverknüpfungen besteht tendenziell ein grosses Missbrauchspotenzial. Gleichzeitig besteht das Risiko, dass dabei eine nicht endende Datensammlung auf Vorrat erstellt wird, indem bereits vorhandenen Daten immer wieder von neuem gespeichert werden und die Aufbewahrungsdauer damit stets verlängert wird. Daher müssen hohe Anforderungen an die Datensicherheit gestellt werden. Bei Datenverknüpfungen ist es besonders wichtig, dass wenn verschiedene Systeme für die Verknüpfung der Daten verwendet wurden, bei allen Systemen die Daten nach einer bestimmten Frist – ab deren Beschaffung – unwiderruflich gelöscht werden. Zur Löschung empfahl die FDS eine Bestimmung aufzunehmen, wonach das verantwortliche Organ periodisch überprüfen muss, ob die beschafften Personendaten noch benötigt werden. Ist das nicht der Fall, müssen sie unverzüglich gelöscht werden.

6.5 Weitere

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

- Mustervertrag Auftragsdatenbearbeitung
- Totalrevision des Gesetzes über Beiträge für familienergänzende Kinderbetreuung
- Revision Universitätsstatut
- Verordnung zum Einführungsgesetz zum Bundesgesetz über die Förderung der Ausbildung im Bereich der Pflege
- Beitritt zur Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung der Informatik in der Strafjustiz
- Verordnung über den Einsatz elektronischer Mittel zur Ton- und Bildübertragung in Zivilsachen
- Schengen-Evaluierung 2025
- Übernahme und Umsetzung der Verordnung (EU) 2022/1190 zur Änderung der Verordnung (EU) 2018/1862 in Bezug auf Informationsausschreibungen im SIS
- Verordnungsanpassungen aufgrund der Übernahme und Umsetzung der Verordnungen (EU) 2021/1133 und (EU) 2021/1134 betreffend das zentrale Visa-Informationssystem

7 Anzeigen

7.1 Zurücksetzen Passwort während Ferienabwesenheit

Eine IT-verantwortliche Person eines öffentlichen Organs liess das Passwort eines Mitarbeitenden desselben öffentlichen Organs beim IT-Dienstleister zurücksetzen und beantragte ein neues Passwort. Das neue Passwort wurde der IT-verantwortlichen Person zugestellt, welche sich in den Account des Mitarbeitenden eingeloggt hat. Zudem lag das neue Passwort während kurzer Zeit offen auf dem Arbeitstisch des abwesenden Mitarbeitenden. Es war unklar, aus welchem Grund das Einloggen erforderlich war. Ferner musste aufgrund der Rückmeldung des IT-Dienstleisters davon ausgegangen werden, dass während der Abwesenheit des Users weitere Logins erfolgt sind. Durch wen, konnte nicht festgestellt werden.

Einsicht und damit Kenntnis in die geschäftlichen Personendaten von Mitarbeitenden sind datenschutzrechtlich nur dann gerechtfertigt, wenn das für die Erfüllung von gesetzlichen Aufgaben erforderlich ist. Lediglich die Funktion als IT-verantwortliche Person berechtigt dazu nicht. Passwörter müssen immer gesichert aufbewahrt und dürfen gegenüber anderen Personen nicht offengelegt werden. Sie sind deshalb in einem verschlossenen Couvert zu überreichen und verschlossen aufzubewahren. Selbst wenn es nur für eine beschränkte Zeit offen für jede Person einsehbar war, bestand während dieser Zeit das Risiko, dass sich eine beliebige unbefugte Person Zugang dazu verschaffen konnte, denn die räumliche Nähe zwischen dem Passwort und dem Arbeitsplatz war durchaus geeignet, den Text als Passwort zu identifizieren. Erlangen unbefugte Personen Kenntnis von diesen Dokumenten, kann dies eine schwerwiegende Beeinträchtigung der Grundrechte der betroffenen Personen mit sich bringen. Die FDS empfahl zudem, den sorgfältigen Umgang mit Personendaten regelmässig zu schulen und die Mitarbeitenden darauf zu sensibilisieren. Beim IT-Dienstleister soll zudem der Prozess für die Zustellung eines neuen Passwortes nochmals überprüft werden.

7.2 Unverschlüsselter Versand und Einwilligungserklärung

Eine Person beschwerte sich, weil ihr ein öffentliches Organ einen Bericht mit Gesundheitsdaten unverschlüsselt per E-Mail zusandte. Das öffentliche Organ verwies auf die unterzeichnete Einwilligungserklärung. Der unverschlüsselte Versand war darin aber nicht aufgeführt. Solch sensible Daten muss ein öffentliches Organ stets verschlüsselt verschicken. Im Einzelfall kann nur dann davon abgewichen werden, wenn die betroffene Person über mögliche Konsequenzen informiert ist und ihre Einwilligung ausdrücklich erteilt hat. Das öffentliche Organ wird inskünftig sämtliche Berichte verschlüsselt über dasselbe Tool verschicken.

8 Einzelanfragen und Medien

8.1 Allgemeines

Wie in jedem Jahr bearbeitete die FDS auch im Berichtsjahr zahlreiche Einzelanfragen und Anfragen von Medien. Erstmals bearbeitete die FDS Auskunfts- und Einsichtsgesuche, welche sie selbst betrafen. Weitere Auskunfts- und Einsichtsgesuche verwies sie an die zuständigen Stellen. Auskunfts- und Einsichtsgesuche müssen jeweils bei derjenigen Stelle gestellt werden, deren Datensammlungen es betrifft.

8.2 Publikationsplattform

Mehrere Personen beschwerten sich darüber, dass ihre Daten auf der Publikationsplattform auffindbar waren. Dies, obwohl beispielsweise Rechtsmittelfristen längstens verstrichen waren oder sich eine Person bei der publizierenden Stelle mit dem Antrag auf Löschung gemeldet hat. Die FDS prüfte die Eingaben und gelangte zur Auffassung, dass der Zweck bzw. die Notwendigkeit der Veröffentlichungen in keinem der Fälle mehr gegeben war. Entweder war die gesetzliche Publikationsfrist abgelaufen oder die Publikation war nicht mehr verhältnismässig, weil nicht mehr erforderlich. Die Fälle betrafen sowohl Gemeinden als auch kantonale Stellen. Weil kein Grund für die weitere Publikation mehr gegeben war, müssen die Angaben gelöscht werden.

Der oben erwähnte Umstand gewinnt an Bedeutung vor dem Hintergrund, dass in der Publikationsplattform eine neue Suchfunktion mit KI eingesetzt wird. Diese findet nicht nur den Suchbegriff selbst, sondern auch semantisch ähnlichen Begriffe. Mit einer solchen Erweiterung ist es umso wichtiger, dass die Publikationsplattform keine unrechtmässigen Einträge enthält. Die FDS empfahl deshalb, die publizierenden Stellen zu informieren und zu sensibilisieren und ein regelmässiges Reporting der nachgesuchten und aufgefundenen Ergebnisse.

8.3 Automatisierte Text-Verarbeitung von Patientenakten

Eine Hochschule wollte im Rahmen eines Forschungsprojekts eine Machbarkeitsstudie zur automatisierten Text-Verarbeitung von Patientenakten bei der Erstellung von medizinischen Gutachten durchführen.

Bei Patientendossiers handelt es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die zudem vom Berufsgeheimnis umfasst werden. Es gelten somit erhöhte Anforderungen an die gesetzliche Grundlage und die Verhältnismässigkeit. Die FDS vertritt die Ansicht, dass eine Bearbeitung von Patientendaten zu Trainingszwecken einer KI oder ähnlichen Systemen ohne explizite gesetzliche Grundlage nicht zulässig ist. Bürgerinnen und Bürger müssen nicht damit rechnen, dass ihre Daten für Trainingszwecke von KI verwendet werden. Dies würde auch dem Grundsatz der Zweckmässigkeit widersprechen. Zudem gehört das Vorhaben zu den Projekten, die vorabkonsultationspflichtig sind.

8.4 Einsatz Azure OpenAI-Technologie

Eine Gesundheitsinstitution stellte die Frage, ob die «Azure OpenAI-Technologie» von Microsoft eingesetzt werden dürfe. Damit soll das Sekretariatspostfach automatisiert werden, um den Arbeitsablauf zu optimieren. Die FDS verwies darauf, dass es sich um ein Vorhaben handelt, das gemäss Merkblatt der FDS der Vorabkonsultation unterliegen dürfte. Bei Personendaten, die einem besonderen Geheimnis unterliegen, wie Daten aus dem Gesundheitsbereich muss sichergestellt werden, dass Microsoft keinen Zugriff auf diese Daten hat. Sie müssen deshalb verschlüsselt werden und das Schlüsselmanagement muss beim öffentlichen Organ liegen.

8.5 Zugriff im Abrufverfahren

Die Finanzkontrolle wandte sich an die FDS mit der Bitte zu beurteilen, ob ein ständiger Zugriff auf das E-Dossier für die Prüfungstätigkeit zulässig sei. Die zuständige Mitarbeiterin benötige einen solchen Zugriff in kürzeren und sehr regelmässigen Abständen.

In diesem Fall handelt es sich um eine Bekanntgabe von besonders schützenswerten Personendaten im Abrufverfahren. Diese ist zulässig, wenn eine formell-gesetzliche Grundlage vorhanden ist. Eine solche liegt derzeit nicht vor. Hingegen beurteilt die FDS den ständigen Zugriff durch die betreffende Mitarbeiterin auf E-Dossier als sinnvoll und zweckmässig. Im Sinn einer vorübergehenden Lösung erachtet es die FDS als vertretbar, dass die Mitarbeiterin für die Erfüllung ihrer gesetzlichen Aufgaben auf die dafür benötigten Angaben Zugriff im Abrufverfahren erhält. Bei der nächsten Gesetzesrevision muss die fehlende Rechtsgrundlage aber geschaffen werden.

8.6 Medienanfragen

Die FDS beantwortete Medienanfragen zu den Themen Videoüberwachung, Lernfördersystem und Datenbekanntgabe.

9 Register und Verzeichnis der Bearbeitungstätigkeit

Die FDS beantwortete verschiedene Anfragen zur Handhabung der Registerführung oder ob eine bestimmte Datensammlung aufgenommen werden müsse. Ein Fall betraf eine vorübergehende Datensammlung. Diese müssen nicht geführt werden, da sie von vornherein nicht auf Dauer ausgelegt sind und nach einer bestimmten Zeit wieder gelöscht werden.

10 Zusammenarbeit und Sensibilisierung

Wie in den vergangenen Jahren pflegte die FDS regelmässigen Austausch mit verschiedenen Stellen beim Kanton, die beim Datenschutz eine wichtige Rolle spielen. Nebst verschiedenen Stellen vor allem im Gesundheits- und Schulbereich u.a. mit der Finanzkontrolle, dem Staatsarchiv, e-Government St.Gallen digital. und dem Fachbereich IT-Recht und Datenschutz bei der Staatskanzlei.

Die Zusammenarbeit mit privatim findet hauptsächlich im Rahmen der Vorstandsarbeit und an den zwei Mal jährlich stattfindenden Plenen statt. Innerhalb des Vorstands übernahm die FDS das Ressort Schulung. Zudem übernahm der IT-Auditor die Leitung einer Arbeitsgruppe von privatim. Die Datenschutzbeauftragten der Ostschweizer Kantone pflegen darüber hinaus einen regelmässigen Austausch über aktuelle Themen.

Auf politischer Ebene wird eine engere Zusammenarbeit der Datenschutzbehörden der Kantone St.Gallen, Thurgau und beider Appenzell angestrebt. Im Berichtsjahr schlossen die vier Kantone eine Vereinbarung ab. Vorgesehen ist eine Zusammenarbeit bei der Digitalisierung und bei kantonsübergreifenden Projekten, z.B. beim Einsatz von M365. Zudem soll die ausserordentliche Stellvertretung – bei einem längeren Ausfall oder bei einem Ausstandsgrund – geregelt werden. Es soll eine juristische Stelle geschaffen werden, welche die Koordination unterstützt. Sie wird beim Kanton Thurgau angesiedelt. Die Umsetzung ist per Mitte 2026 vorgesehen.

Die FDS ist gut aufgestellt und verfügt sowohl über juristisches als auch IT-Know-how. Dennoch begrüsst sie eine engere Zusammenarbeit bei Themen, die alle vier Kantone betreffen. Wichtig ist, dass die gesetzlich vorgesehene Unabhängigkeit vollumfänglich gewahrt bleibt. Zudem muss im Auge behalten werden, wie sich der Aufwand für die Koordination entwickelt. Zwar dürfte die juristische Stelle teilweise eine Entlastung bei gemeinsamen Themen bringen, die Koordination und Abstimmung liegt aber bei den einzelnen Datenschutzbehörden und nicht bei der juristischen Stelle. Auch ist derzeit unklar, wie gross der Umfang an gemeinsamen Themen ist.

Wie jedes Jahr erarbeitete die FDS eine Sequenz für das E-Learning Datenschutz und IT-Sicherheit des Kantons. Thema war die Qualifizierung der verschiedenen Arten von Personendaten. Zudem fand eine Informationsveranstaltung zum Datenschutz beim Bau- und Umweltdepartement statt. Im Jahr 2025 soll ausserdem ein «Self-Check» für die öffentlichen Organe fertig gestellt werden. Damit sollen die öffentlichen Organe ihre «Datenschutz-Fitness» testen können.

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

11 Personelles und Ressourcen

Seit April des Jahres 2023 verfügt die FDS über einen IT-Auditor. Die FDS ist fachlich somit gut aufgestellt mit einem interdisziplinären Team, das gut eingespielt ist. Das ist im Zeitalter der Digitalisierung unentbehrlich, weil ausserhalb der Rechtsetzung die meisten Geschäfte der FDS Fragen der Informationssicherheit beinhalten. Es ist aber auch erforderlich, um den stets gestiegenen Anforderungen an die Unabhängigkeit gerecht zu werden.

Die Arbeitsbelastung bleibt hoch. Zwar hat die Fallzahl gegenüber dem Vorjahr etwas abgenommen. Wie bereits in den Vorjahren ausgeführt, ist aber nicht mehr die Anzahl, sondern die Komplexität der Fälle entscheidend für die Arbeitsintensität. Die Art der Aufgaben hat sich seit der Revision des Datenschutzgesetzes im Jahr 2019 verändert, weg von der Einzelanfrage hin zu komplexeren, weniger einzelfallbezogenen Aufgaben. Viel Zeit beanspruchen die Vorabkonsultationen. Einerseits hängt das mit der Anzahl der Eingänge zusammen, anderseits aber auch mit der grossen Komplexität vor allem der Vorhaben mit hohem Risiko. Die gesetzliche Frist für deren Bearbeitung ist mit maximal sechs Wochen sehr kurz, auch im interkantonalen und internationalen Vergleich. Diese Kombination führt angesichts des kleinen Teams teilweise zu zeitlichen Engpässen, die nicht immer einfach zu bewältigen sind. Eine vertiefte Auseinandersetzung mit dem ganzen Projekt ist so teilweise nicht möglich und es muss strikt priorisiert werden.

12 Prüfprogramm 2025

Die FDS legt für das Jahr 2025 folgendes Prüfprogramm fest:

- Schuladministrationssoftware NESA
- Klinikinformationssystem KISIM
- Publikationsplattform (technische Prüfung)
- Arbeitsbesuch bei einer Gemeindefachstelle für Datenschutz[13]

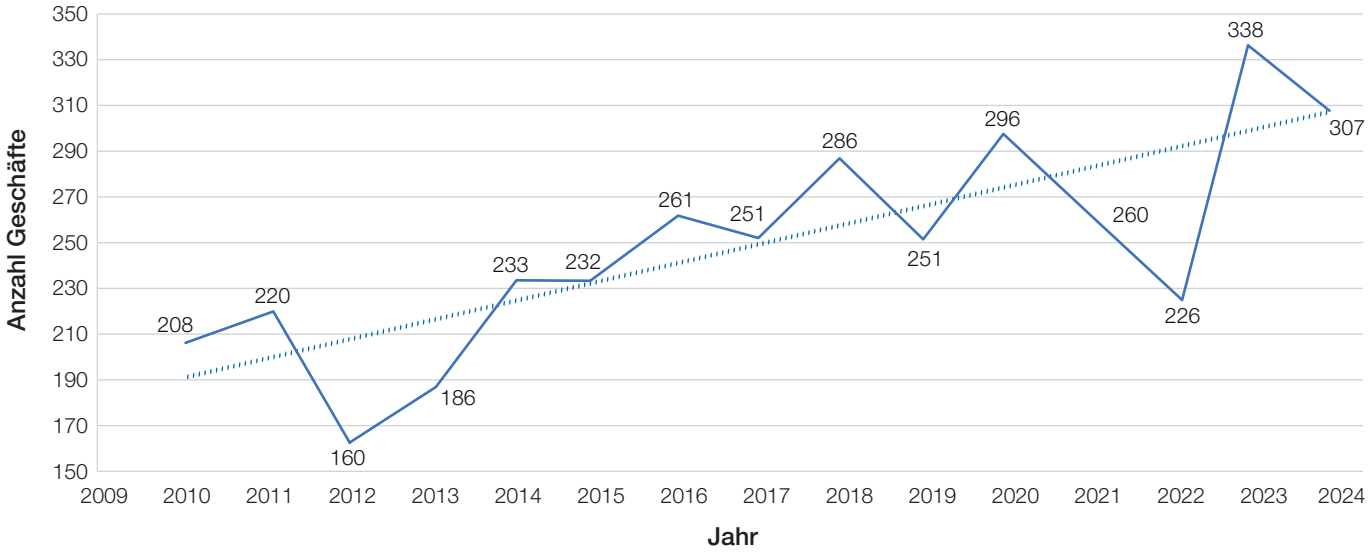
13
Siehe dazu Ausführungen in Ziff. 4.2.

13 Antrag

Wir beantragen Ihnen, Frau Präsidentin, sehr geehrte Damen und Herren, auf den vorliegenden Bericht einzutreten.

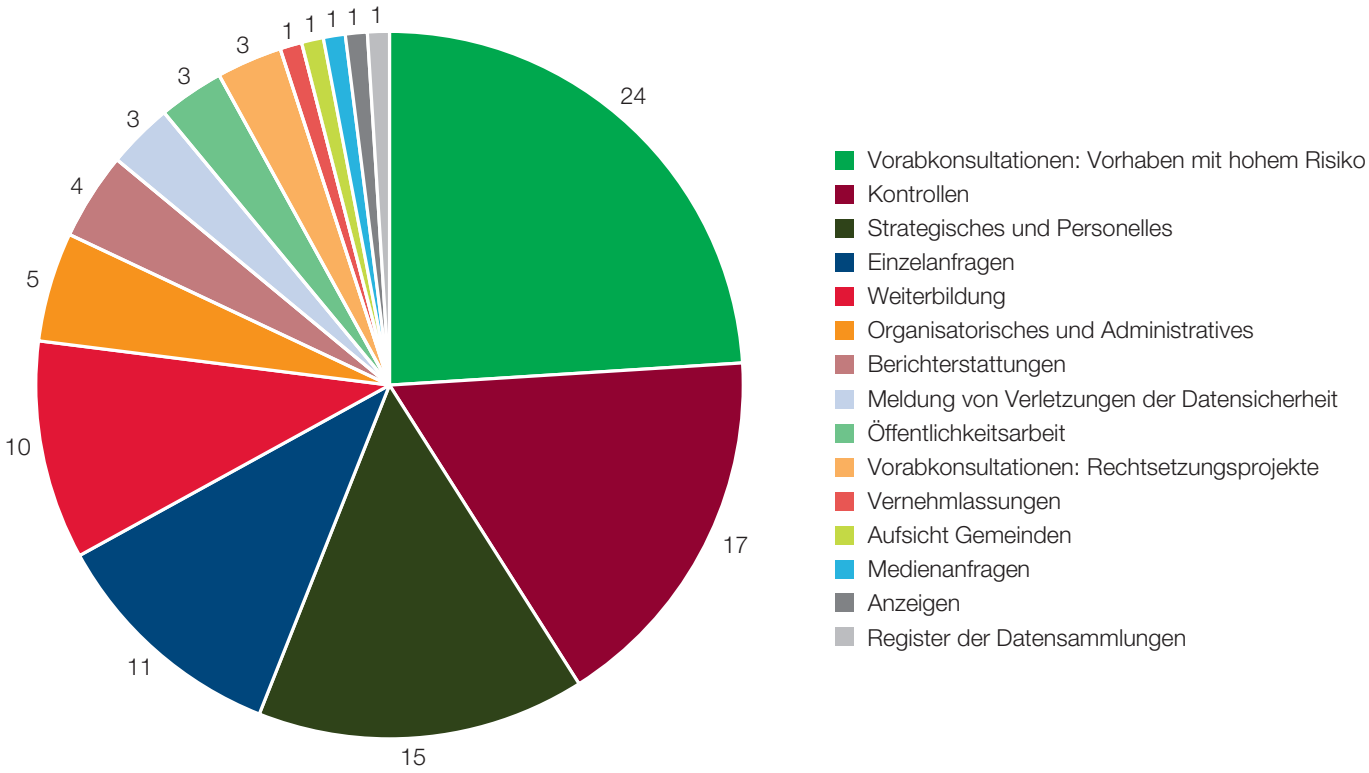
Kantonale Fachstelle für Datenschutz
Corinne Suter Hellstern, Leiterin

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), 2024

Kantonsrat des Kantons St.Gallen
Geschäft 32.25.03

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