Kanton St.Gallen
Fachstelle für Datenschutz

Bericht der kantonalen Fachstelle für Datenschutz über das Jahr 2023



Inhaltsverzeichnis

Zusammenfassung 4

1 Einführung 6

2 Prüftätigkeit 7

2.1 Lernfördersysteme 7
2.2 Geschäftsverwaltungssystem des Kantons 9
2.3 Patientenportal 10
2.4 Pupil Messenger 11
2.5 Pensionskasse 11
2.6 Geoportal 11
2.7 Zugriffe auf Kantonale Einwohnerdatenplattform 11

3 Meldungen Verletzung Datensicherheit 12

3.1 XPlain 12
3.2 Falsche Postzustellung 12
3.3 Unzulässige Datenbekanntgaben 13

4 Aufsicht und Beratung Gemeindefachstellen 14

4.1 Arbeitsbesuch 14
4.2 Erfahrungsaustausch 15
4.3 Leistungsvereinbarung IT-Audit 15

5 Vorhaben mit hohem Risiko 16

5.1 Videoüberwachung Amt 16
5.2 Videoüberwachung Spital 17
5.3 M365 17
5.4 wir.impfen.ch 18

6 Rechtsetzung 19

6.1 Automatisierte Fahrzeugfahndung 19
6.2 Grundbuchverordnung 19
6.3 Strafprozessverordnung 20
6.4 Videoüberwachung 20
6.5 Merkblatt KI 21
6.6 Weitere Stellungnahmen 21

7 Anzeigen 22

8 Einzelanfragen und Medien 23
8.1 Allgemeines 23
8.2 Darmkrebsprogramm 23
8.3 Gesetzliche Grundlage Archivierung Patientendossier 23
8.4 Datenschutzerklärungen auf Webseiten 23

9 Register und Verzeichnis der Bearbeitungstätigkeit 24

10 Zusammenarbeit und Sensibilisierung 25

11 Leistungsvereinbarung Bistum St.Gallen 26

12 Personelles und Ressourcen 26

13 Prüfprogramm 2024 26

14 Antrag 26

Anhang – Zahlen 27

Zusammenfassung

Die grosse und weiter zunehmende Komplexität beim Datenschutz begleitete die Fachstelle für Datenschutz (FDS) auch im Jahr 2023, etwa bei Fragen zu E-Government-Projekten oder Auftragsdatenbearbeitungen. Auch die Videoüberwachung war einmal mehr Thema. Einerseits nahm die FDS Stellung zum Gesetzesentwurf, anderseits beurteilte sie zwei Vorhaben. Aufgrund der gesetzlichen Ausgangslage im Kanton ist eine Videoüberwachung nur in einem sehr eng begrenzten Rahmen möglich. Zudem handelt es sich auch bei einer Echtzeit-Beobachtung ohne Aufzeichnung um eine Videoüberwachung. Ein solcher Einsatz muss ebenfalls die Voraussetzungen an die Einschränkung eines Grundrechts erfüllen. Bei Vorhaben betreffend Videoüberwachung ist die FDS der Ansicht, dass es generell eine Vorabkonsultation – eine vorgängige Prüfung durch die FDS – braucht. Dies, weil es derzeit keine gesetzliche Grundlage für Videoüberwachung durch öffentliche Organe gibt.

Im Jahr 2023 schloss die FDS die Prüfung der Lernfördersysteme ab. Es handelt sich um ein digitales, adaptives Übungs-, Förder- und Testtool. Adaptiv heisst, dass sich das System an das Lern-Niveau der Schülerinnen und Schüler anpasst und je nachdem andere Fragen stellt. Dabei werden sensible Daten von Schülerinnen und Schülern bearbeitet. Die FDS machte verschiedene Empfehlungen, vor allem zur Auftragsdatenbearbeitung: Solche Daten sollten nicht in einem Land mit einem nicht angemessenen Datenschutzniveau bearbeitet werden. Ansonsten müssen die Personendaten verschlüsselt werden und das Schlüsselmanagement muss beim öffentlichen Organ liegen. Weiter schloss die FDS die Prüfung des Geschäftsverwaltungssystems des Kantons (GEVER) ab. Das Augenmerk lag bei den im System bearbeiteten Personendaten und der Organisation: Personaldaten sollten im speziell dafür vorgesehenen System bearbeitet werden und nicht in GEVER. Die im Amt für GEVER verantwortlichen Personen haben umfassende Zugriffe auf sehr sensible Daten. Entsprechend sorgfältig müssen sie ausgewählt und geschult werden.

XPlain war im Berichtsjahr Thema in den Medien. Es geht um eine Hacker-Gruppierung, die sich Zugriff auf die Infrastruktur des Schweizer Software-Unternehmens XPlain verschaffte. Auch die Kantonspolizei St.Gallen war davon betroffen. Wie die Abklärung ergab, war sie allerdings nur am Rand betroffen. Sensible Personendaten waren nicht tangiert. Weitere Meldungen von Datenschutzverletzungen betrafen meistens unzulässige Datenbekanntgaben.

Die FDS machte einen Arbeitsbesuch bei der Fachstelle für Datenschutz der Stadt St.Gallen. Die Stelle ist bei der Finanzkontrolle angegliedert und verfügt über ein Pensum von 30 Prozent. Dies erachtet die FDS als zu wenig. Mit einer anderen organisatorischen Ausgestaltung könnte zudem die Unabhängigkeit der Stelle gestärkt werden.

Die FDS äusserte sich zur automatisierten Fahrzeugfahndung. Es war vorgesehen, die Fahrzeuginsassinnen und -insassen bildlich zu erfassen. Damit entstünde eine sehr umfassende Datensammlung, die sehr viele Personen betrifft und dies ohne Anfangsverdacht. Die FDS ist der Ansicht, dass auf die bildliche Erfassung verzichtet werden sollte.

Die FDS bearbeitete zahlreiche Anfragen. Themen waren das Darmkrebsprogramm, die gesetzliche Grundlage für die Archivierung von Patientendossiers und Datenschutzerklärungen auf Webseiten.

Im Berichtsjahr konnte die FDS eine Stelle IT-Audit besetzen. Bisher arbeitete die FDS eng mit dem Dienst für Informatikplanung (DIP) zusammen. Die Stelle bei der FDS bedeutet eine Stärkung der Unabhängigkeit. Weil die Gemeindefachstellen für Datenschutz nicht über ein entsprechendes Know-how verfügen, schlossen sie mit der FDS Leistungsvereinbarungen ab. Nach Bedarf können sie so entsprechendes Wissen einkaufen.

Schliesslich schloss die FDS mit dem Bistum St.Gallen eine Leistungsvereinbarung über die Gewährleistung der Aufgaben im Bereich Datenschutz ab. Eine vergleichbare Vereinbarung hat die FDS mit dem Katholischen Konfessionsteil bereits im Jahr 2020 abgeschlossen.

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 2023.

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 Einführung

Die grosse und weiter zunehmende Komplexität begleitete die FDS auch im Jahr 2023, beispielsweise bei E-Government-Projekten. In diese sind verschiedene Staatsebenen involviert. Es stellen sich Fragen der Zuständigkeiten und Verantwortlichkeiten. Die Beantwortung dieser Fragen ist für die Einhaltung der Datenschutzbestimmungen essenziell. Aber auch die zahlreichen Auftragsdatenbearbeitungen sind komplex, nicht nur, weil sie in der Cloud stattfinden. Häufig bestehen Unterauftragsdatenbearbeitungen; Teilweise in Konstellationen in denen fraglich ist, ob das öffentliche Organ noch abschätzen kann, welches Risiko es trägt. Sind Auswirkungen auf die Privatsphäre der betroffenen Personen möglich, muss es dies aber einschätzen können. Das öffentliche Organ bleibt nämlich für das Vorhaben verantwortlich.

Im Berichtsjahr befasste sich die FDS mit Fragen im Zusammenhang mit der Meldepflicht bei Datenschutzvorfällen. Diese Pflicht wurde neu mit dem revidierten Datenschutzgesetz eingeführt. In bestimmten Fällen ist das öffentliche Organ verpflichtet, der FDS eine solche Meldung zu machen. Das ist der Fall, wenn ein potentiell hohes Risiko für die Privatsphäre der betroffenen Personen besteht. Wenn die FDS nun feststellt, dass es sich nicht um ein hohes Risiko handelt – kann sie trotzdem Empfehlungen machen? Kann sie verlangen, dass die betroffenen Personen informiert werden? Die FDS bejahte diese beiden Fragen. Andere Fragen im Zusammenhang mit der Meldepflicht stellen sich zur interkantonalen Zusammenarbeit: Immer mehr Fälle betreffen Software, die von verschiedenen Kantonen verwendet wird. Darf die FDS die anderen Kantone informieren? Oder muss sie sogar? Weil sich diese Fragen nicht nur der FDS des Kantons St.Gallen stellen, werden sie im Rahmen von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, behandelt.

Auch Videoüberwachungen waren im Berichtsjahr einmal mehr Thema. Nach wie vor gibt es keine formell-gesetzliche Grundlage für die Videoüberwachung durch kantonale Stellen. Deshalb ist eine Videoüberwachung nur in einem sehr eng begrenzten Rahmen möglich: Sie muss für die gesetzliche Aufgabenerfüllung unentbehrlich sein. D.h., dass das öffentliche Organ die gesetzliche Aufgabe nicht mehr ordnungsgemäss erfüllen kann, etwa, weil die Sicherheit von Mitarbeitenden schwerwiegend beeinträchtigt ist. Es müssen also bereits Vorkommnisse vorliegen. Auch ist es das letzte Mittel, um die gesetzliche Aufgabenerfüllung sicherstellen zu können. Gibt es mildere Massnahmen, ist eine Videoüberwachung nicht verhältnismässig. Wichtig ist zudem, der FDS solche Vorhaben zur Vorabkonsultation vorzulegen. Die FDS legt in solchen Fällen an die Pflicht einer Vorabkonsultation einen strengeren Massstab an. Gerade weil keine formell-gesetzliche kantonale Grundlage vorliegt, ist die FDS der Ansicht, dass es umso wichtiger ist, dass die datenschutzrechtliche Vereinbarkeit vorab geprüft wird.

2 Prüftätigkeit

2.1 Lernfördersysteme

Im Jahr 2022 prüfte die FDS die Lernfördersysteme für die Volksschule (LFS) des kantonalen Lehrmittelverlags. Die Prüfung konnte im Berichtsjahr abgeschlossen werden. Bei den LFS handelt es sich um ein digitales adaptives Übungs-, Förder- und Testtool. Adaptiv heisst, dass je nach Lern-Niveau der Schülerinnen oder Schüler andere Fragen gestellt werden. Die LFS bezwecken die Unterstützung von Lernenden und das individuelle Lernen und Fördern der Schülerinnen und Schüler. Der Lehrmittelverlag St.Gallen ist produzierender Verlag der LFS. Stellwerk, ein Testsystem zum Prüfen des Wissens von Schülerinnen und Schülern in bestimmten Bereichen und Teil der LFS ist für die 8. Klassen im Kanton St.Gallen obligatorisch. Die LFS werden nicht nur von Schulen im Kanton St.Gallen, sondern von Schulen der gesamten Deutschschweiz genutzt.

Der Lehrmittelverlag hat die Datenbearbeitung an Dritte ausgelagert. Der Sitz des Auftragsdatenbearbeiters ist in der Schweiz, Wohnsitz des Inhabers und der Mitarbeitenden sind aber in einem Land mit einem nicht angemessenen Datenschutzniveau gemäss Länderliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)[4]. Zum Zeitpunkt der Prüfung hatten diese Personen sowohl auf das produktive System als auch auf die archivierten Personendaten Zugriff. Der Lehrmittelverlag beabsichtigte, selbst und ausschliesslich über Schlüssel und Schlüsselmanagement zu verfügen.

4
Verordnung über den Datenschutz, SR 235.11, Anhang 1.

Die bearbeiteten Personendaten werden nicht gelöscht bzw. vernichtet und auch nicht dem Archiv angeboten. Begründet wird dies damit, dass ein Kernelement der LFS der soziale Vergleich sei. Dieser solle über den Zeitraum der vergangenen 20 Jahre ermöglicht werden. Lehrpersonen haben vier Jahre nach dem Zeitpunkt der Stellwerk-Prüfung keinen Zugriff mehr auf die Personendaten. Eine Hochschule hat regelmässig Zugriff auf die Datensammlung, um daraus Erkenntnisse für die Forschung abzuleiten.

Weil die LFS aus einer Zeit stammen, in der Datenschutz und Datensicherheit kaum Thema waren und über die Jahre gewachsen sind, wurde diesen Aspekten bisher eher wenig Beachtung geschenkt. Die FDS machte Empfehlungen v.a. zur Auftragsdatenbearbeitung und Aufbewahrung.

Bei den in den LFS bearbeiteten Personendaten handelt es sich nach Ansicht der FDS um ein Profiling gemäss Datenschutzgesetz. Zudem werden Daten von Schülerinnen und Schülern der obligatorischen Volksschule bearbeitet. Einerseits ist die Bearbeitung von Daten von Jugendlichen besonders sensitiv, anderseits ist der Stellwerk-Test obligatorisch, die Jugendlichen können sich dem nicht entziehen. Für die Lehrstellensuche und damit die berufliche Zukunft der Jugendlichen ist der Stellwerk-Test sehr wichtig, was besondere Anforderungen an die Integrität des Ergebnisses stellt. Eine Beeinträchtigung der rechtmässigen Bearbeitung solcher Daten birgt eine besonders hohe Gefahr einer schwerwiegenden Verletzung der Persönlichkeit, dementsprechend hoch müssen Datenschutz und Datensicherheit gewichtet werden.

Profilings sollten nicht in einem Land mit einem nicht angemessenen Datenschutzniveau bearbeitet werden. Ist das nicht anders möglich, weil beispielsweise nur dieser Anbieter entsprechende Anwendungen führt, müssen die Daten verschlüsselt werden und der Schlüssel muss beim öffentlichen Organ liegen. Der Lehrmittelverlag sicherte anlässlich der Prüfung zu, dass dies umgesetzt würde. Die FDS erachtete diese Massnahme als vordringlich. Per Ende 2023 hat der Lehrmittelverlag die Empfehlung umgesetzt.

Das öffentliche Organ muss grundsätzlich sicherstellen, dass Auftragsdatenbearbeiter vertrauenswürdig sind. Die gewählten organisatorischen Lösungen sollten zudem nicht so komplex sein, dass kein Überblick mehr besteht und das öffentliche Organ die Verantwortung dafür gar nicht mehr übernehmen kann. Sämtliche datenschutzrechtlichen Fragen sind ausserdem im Vorfeld einer Auslagerung zu prüfen. Der mit dem Auftragsdatenbearbeiter abgeschlossene Vertrag muss alle datenschutzrechtlichen Anforderungen erfüllen.[5]

5
Siehe dazu Merkblatt Auftragsdatenbearbeitung.

Für die Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken gelten nach dem DSG erleichterte Voraussetzungen. Dies deshalb, weil der Zweck der Bearbeitung nicht bei den Personen als solches liegt, sondern die Personendaten «lediglich» unabdingbar sind, um andere Aufgaben erfüllen zu können im Bereich Forschung, Planung und Statistik. Im Vorfeld einer konkreten Anfrage muss aber geprüft werden, ob für die Aufgabenerfüllung Personendaten notwendig sind oder ob anonymisierte Daten genügen. Zudem muss auch in jedem einzelnen Fall geprüft werden, ob für den angegebenen Zweck eine Datenbekanntgabe zulässig ist. Wichtig ist auch, alle datenschutzrechtlichen Modalitäten in der Vereinbarung mit der Hochschule zu regeln.

Personendaten müssen nach einer definierten Frist entweder dem Staatsarchiv angeboten oder vernichtet werden. Eine «ewige» Aufbewahrung ist datenschutzrechtlich ohne gesetzliche Grundlage nicht zulässig, auch nicht für Forschungsvorhaben. Für ein Monitoring braucht es keine Personendaten. Sollen die Personendaten nach der definierten Aufbewahrungsdauer dafür länger aufbewahrt werden, müssen sie anonymisiert werden. Dann kann auch auf die Vernichtung verzichtet werden. Eine Verschlüsselung hingegen würde nicht ausreichen, da es sich auch bei verschlüsselten Daten potentiell immer noch um Personendaten handelt. Jemand besitzt den Schlüssel für die Entschlüsselung.

Bei der Informationssicherheit empfahl die FDS die Anwendung als geheim zu klassifizieren und mit dem Betreiber zu vereinbaren, dass die Datensicherungen regelmässig überprüft werden.

2.2 Geschäftsverwaltungssystem des Kantons

Ende 2022 prüfte die FDS Organisation und Zugriffsberechtigungen des elektronischen Geschäftsverwaltungssystems (GEVER) des Kantons. Das System unterstützt die Mitarbeitenden, Geschäfte zur Erfüllung von gesetzlich geregelten Aufgaben bzw. alle dazugehörigen Dokumente (Office, E-Mail, Scans etc.) in einem entsprechenden Dossier abzulegen und über den ganzen Lebenszyklus hinweg zu bewirtschaften. Es werden sämtliche geschäftsrelevanten Dokumente einer Verwaltungsakte zentral abgelegt. GEVER wird bis Mai 2024 schrittweise in der Zentralverwaltung, der Staatsanwaltschaft und bei den Gerichten eingeführt.

Die Fachstelle GEVER ist für den fachlichen und technischen Betrieb des Systems, Organisation, Koordination und die Vermittlung von Know-how zuständig. Sie ist organisatorisch bei der Staatskanzlei angesiedelt. In jedem Amt gibt es GEVER-Verantwortliche, die für definierte Aufgaben im Zusammenhang mit GEVER beim Amt zuständig sind. Es handelt sich meist um Mitarbeitende der Administration, IT-Fachpersonen oder Stabsmitarbeitende. Diese Mitarbeitende kennen die Organisation und die eingesetzten Mittel. GEVER-Verantwortliche haben auf sämtliche Dossiers ihres Amtes Zugriff, um ihre Unterstützungsaufgabe wahrnehmen zu können.

GEVER wird in Auftragsdatenbearbeitung betrieben. Die Modalitäten sind in einem Rahmen- und einem Betriebsvertrag geregelt.

Nebst «gewöhnlichen» werden auch besonders schützenswerte Personendaten bearbeitet: einerseits betrifft das die Bearbeitung von Kerngeschäften in GEVER. Anderseits werden teilweise auch Daten z.B. aus dem Personalwesen bearbeitet, für die es spezielle Applikationen gibt (eDossier). Grund für die Bearbeitung von Personalgeschäften in GEVER ist, dass das eDossier keine Bearbeitung von Dokumenten zulässt und oft auch die Zugriffsberechtigungen fehlen.

Die Berechtigungen erteilt die GEVER-Fachstelle zentral. Nach Ablauf der Aufbewahrungsfrist werden die Dossiers dem Staatsarchiv abgeliefert oder vernichtet.

Der GEVER-Fachstelle ist die Sensibilität des Themas Datenschutz bewusst. Die FDS begrüsst, dass die Fachstelle GEVER die Vergabe der Zugriffsrechte zentralisiert hat. So kann eine einheitliche Handhabung sichergestellt werden und es findet eine Plausibilisierung statt. Empfehlungen machte die FDS bei der Art der in GEVER bearbeiteten Personendaten: Personaldaten, für welche es eine eigene Applikation gibt, sollten nicht in GEVER bearbeitet werden. Sie sollten inskünftig im e-Dossier bearbeitet werden können.

Ein besonderes Augenmerk ist auf die GEVER-Verantwortlichen in den Departementen zu legen. Sie haben umfassende Zugriffe auf sämtliche in GEVER bearbeiteten Daten des Amtes. Bereits bei der Auswahl der verantwortlichen Personen sollte darauf geachtet werden, dass sie für den Datenschutz sensibilisiert sind. Es sollten zudem Personen berücksichtigt werden, die aufgrund ihrer Funktion bereits einen umfassenden Zugriff auf viele in GEVER bearbeitete Daten haben. So erhalten nicht zusätzliche Personen Kenntnis von sensiblen Daten. Insbesondere die Zugriffe auf besonders schützenswerte Personendaten sollten regelmässig kontrolliert werden. Zudem sollten regelmässige Sensibilisierungen stattfinden. Bei internen Stellenwechseln muss darauf geachtet werden, dass die Zugriffsberechtigungen entzogen werden.

Angesichts der allgemein immer häufigeren und teils schwerwiegenden Verletzungen der Datensicherheit muss das öffentliche Organ die Verantwortlichkeiten bei einem Vorfall festlegen, damit rasch gehandelt werden kann. Es muss sichergestellt werden, dass überfällige Dossiers dem Staatsarchiv abgeliefert und die nicht abgelieferten Unterlagen (inkl. Backups u.Ä.) vernichtet werden.

Mit dem Auftragsdatenbearbeiter sollte der Beizug von Subunternehmern geregelt werden, auch wenn derzeit nicht die Absicht besteht, solche beizuziehen. Bei einem Vorfall ist der Auftragsdatenbearbeiter gesetzlich verpflichtet, dies dem öffentlichen Organ unverzüglich zu melden. Zusätzlich sollte das im Auftragsdatenbearbeitungsvertrag festgehalten werden.

Bei den Teamräumen muss ein Augenmerk auf der Vergabe und dem Entzug von Berechtigungen sowie der Möglichkeit des Teilens von entsprechend klassifizierten Dokumenten liegen. Die Dokumente müssen mit organisatorischen und technischen Massnahmen angemessen geschützt werden. Zudem dürfen sie nur mit einem spezifizierten Personenkreis im Internet geteilt werden. Die FDS empfahl ausserdem, dass ein Sicherheitsaudit gemacht werden soll. Die für GEVER Verantwortlichen beschlossen, dass der Co-Work Teamraum vorerst nicht ausgebreitet wird, zudem soll im Jahr 2024 ein Sicherheitsaudit durchgeführt werden.

2.3 Patientenportal

Die FDS hat im Berichtsjahr das Patientenportal bei einem Spital geprüft. Themen waren u.a. Verantwortlichkeiten, Rechte der Patientinnen und Patienten, Registrierungsprozess, Zugriffsberechtigungen und Aufbewahrung.

Das Portal macht einen soliden Eindruck. Die FDS machte ein paar Empfehlungen zum Registrierungsprozess, zur Aufbewahrungsdauer sowie zur Schulung von Mitarbeitenden. Zudem wies sie auf die Pflicht hin, die Datensammlungen künftig im Register der Datensammlungen zu führen.

2.4 Pupil Messenger

Die FDS prüfte Pupil Messenger im Herbst des Berichtsjahres. Der Pupil Messenger ist Teil des Projekts «Pupil», eine Schulverwaltungssoftware. Er dient den Schulgemeinden für die Kommunikation mit den Eltern. Weil die datenschutzrechtliche Aufsicht über die Schulgemeinden bei den Gemeindefachstellen für Datenschutz liegt, werden auch diese in die Prüfung involviert. Die Prüfung ist noch nicht abgeschlossen.

2.5 Pensionskasse

Die FDS prüfte Datenschutz und IT-Sicherheit bei der St.Galler Pensionskasse (sgpk) Ende des Berichtsjahres. Als kantonales öffentliches Organ fällt sie in den Geltungsbereich des DSG[6]. Ein erster Teil der Prüfung soll im ersten Semester 2024 abgeschlossen werden. Im Bereich der IT-Sicherheit bestehen Abhängigkeiten zu kantonalen Vorgaben, die derzeit geändert werden. Der Abschluss dieser Prüfung ist deshalb davon abhängig, wann die nötige Dokumentation zur Verfügung steht.

6
Siehe Tätigkeitsbericht über das Jahr 2022, Ziff. 7.3.

2.6 Geoportal

Das Geoportal war bei der FDS bereits in den Jahren 2021 und 2022 Thema. Die zuständige Stelle machte damals eine Datenschutz-Folgenabschätzung, die kein hohes Risiko für das Projekt ergab.

Zu einem späteren Zeitpunkt war vorgesehen, Microsoft als Betreiberin des Rechenzentrums zu beauftragen. Das öffentliche Organ vereinbarte mit Microsoft, dass Schlüssel und Schlüsselmanagement beim öffentlichen Organ verblieben. Somit hat Microsoft keinen Zugriff auf die Personendaten. Zwar veränderte sich damit die Ausgangslage, das Risiko war mit der gewählten Lösung aber nach wie vor nicht als hoch einzuschätzen. Weil die Arbeiten zu diesem Projekt noch in Gang waren und angesichts des nach wie vor als nicht hoch eingeschätzten Risikos verzichtete die FDS auf eine Prüfung.

2.7 Zugriffe auf Kantonale Einwohnerdatenplattform

Mit der Kantonalen Einwohnerdatenplattform (KEWR) werden Personendaten von Bürgerinnen und Bürgern nicht mehr aktiv von der Gemeinde an eine kantonale Stelle bekannt gegeben. Die Mitarbeitenden des Kantons können sie von sich aus abrufen. Es ist deshalb wichtig, dass die berechtigten Stellen nur auf diejenigen Personendaten zugreifen können, die sie für ihre gesetzliche Aufgabenerfüllung wirklich benötigen. Im Berichtsjahr hat die FDS stichprobenweise die Zugriffsberechtigungen zweier Stellen im Bau- und Umweltdepartement geprüft. Die FDS prüfte einerseits, ob rechtliche Grundlagen vorhanden sind, welche die Bearbeitung dieser Personendaten rechtfertigen. Andererseits prüfte sie, ob diese Personendaten für den Geschäftsprozess notwendig sind. Weiter wurde die organisatorische Handhabung geprüft. Der FDS erschienen die Zugriffe auf KEWR mehrheitlich plausibel. Gesamthaft betrachtet machte die Handhabung bei den geprüften Stellen einen guten Eindruck.

3 Meldungen Verletzung Datensicherheit

3.1 XPlain

Im Berichtsjahr war die Datenschutzverletzung XPlain in den Medien. Eine Hacker-Gruppierung namens «PLAY» verschaffte sich Zugriff auf die ICT-Infrastruktur des Schweizer Software-Unternehmens Xplain AG. Anschliessend veröffentlichte sie Daten im Darknet. Im Kanton St.Gallen war vorab die Kantonspolizei (Kapo) betroffen. Im Vergleich zu anderen Kantonen allerdings nur in vergleichsweise geringem Ausmass, sowohl was die Menge als auch die Art der betroffenen Personendaten anbelangte. Gemäss Schilderung der Kapo war einzig ein Protokoll einer Sitzung mit dem Unternehmen betroffen. Gegenstand der Besprechung waren betriebliche Angelegenheiten. Diese können durchaus heikel sein, i.d.R. aber weniger in datenschutzrechtlicher Hinsicht. Das hängt vom Gegenstand der Sitzung und den konkreten Voten ab. Aufgrund der Schilderung der Kapo teilte die FDS die Ansicht, dass es sich nicht um besonders schützenswerte Personendaten handelt. Die Art der Datenschutzverletzung hat zwar ein grosses Potential für eine schwerwiegende Verletzung der Grundrechte der betroffenen Person. Allerdings waren nur wenige Personen in einem datenschutzrechtlich weniger heiklen Bereich betroffen. Somit dürfte auch die Schwere der Folgen für die betroffenen Personen nicht sehr gross sein. Die Kapo hatte die betroffenen Personen bereits informiert, womit sich diese Frage nicht mehr stellte.

3.2 Falsche Postzustellung

Ein öffentliches Organ war damit konfrontiert, dass verschiedentlich für eine Arztpraxis bestimmte Post einer privaten Person, die im selben Haus wohnte, zugestellt wurde. Die Art der bearbeiteten Personendaten gehören zu den besonders schützenswerten und unterstehen einem besonderen Amtsgeheimnis. Die betroffene Stelle hat verschiedene Massnahmen getroffen: Sie hat die zuständigen Mitarbeitenden sensibilisiert, beim Versand den Vermerk «Vertraulich» angebracht und die gespeicherte Adresse präzisiert.

Besteht bei einer Datenschutzverletzung ein hohes Risiko für die Grundrechte der betroffenen Personen, muss das öffentliche Organ den Vorfall der FDS melden. Angesichts der Art und des Zwecks der bearbeiteten Personendaten bejahte die FDS die Meldepflicht. Nach Ansicht der FDS mussten die betroffenen Personen aber nicht informiert werden, weil sie keine Möglichkeit hatten, die Risiken für ihre Persönlichkeit und Grundrechte selbst zu reduzieren. Sie konnten keine eigenen Vorkehrungen zu ihrem Schutz treffen. Nebst denjenigen Massnahmen, die das öffentliche Organ bereits ergriffen hat, empfahl die FDS der Post mitzuteilen, dass in der Vergangenheit Briefe wiederholt fehlerhaft zugestellt worden seien. Es solle darauf geachtet werden, dass dies inskünftig vermieden werde.

3.3 Unzulässige Datenbekanntgaben

Häufig sind unzulässige Datenbekanntgaben Gegenstand von Meldepflichten. Ein öffentliches Organ stellte der Arbeitgeberin einer betroffenen Person Unterlagen mit besonders schützenswerten Personendaten zu. Dabei stellte das öffentliche Organ vorgängig nicht sicher, dass die Unterlagen nur von der dafür bestimmten Person bei der Arbeitgeberin entgegengenommen werden konnten. Auch innerhalb einer Software-Anwendung können falsche oder zu wenig strikte Zugriffsberechtigungen zu unzulässigen Datenbekanntgaben führen. In einem Fall wurden die Zugriffsberechtigungen von einem Auftragsdatenbearbeiter falsch vergeben.

Je nach Art und Umfang der Daten sowie dem Kontext können Folgen solcher unzulässiger Datenbekanntgaben Identitätsdiebstahl, Reputationsschaden oder eine Geheimnisoffenbarung sein. Auch wenn es sich bei den einzelnen Personendaten nicht um besonders schützenswerte handelt, kann die Kombination aller Angaben unter Umständen heikel sein und hohe Risiken nach sich ziehen. Allerdings bergen nicht alle unzulässigen Datenbekanntgaben ein hohes Risiko und sind somit meldepflichtig: ein falsch zugestelltes Mail mit terminlichen Angaben zu einem Projekt führt normalerweise nicht zu einem hohen Risiko für betroffene Personen.

4 Aufsicht und Beratung Gemeindefachstellen

4.1 Arbeitsbesuch

Im Berichtsjahr stattete die FDS der Fachstelle für Datenschutz der Stadt St.Gallen (nachfolgend FS) einen Arbeitsbesuch ab. Die FS ist bei der Finanzkontrolle angegliedert. Diese ist unabhängig und administrativ dem Stadtrat zugeordnet. Die Leiterin der FS nimmt zusätzlich Aufgaben in der Revision und weitere Aufgaben der Finanzkontrolle wahr. Für die Funktion der FS stehen 30 Stellenprozente zur Verfügung. Internes IT-Know-how ist nicht vorhanden. Es besteht aber eine enge Zusammenarbeit mit den Informatik-Diensten der Stadt St.Gallen, vor allem mit dem Informationssicherheitsbeauftragten.

Mit 30 Stellenprozenten ist der FS eine umfassende Erfüllung der gesetzlichen Aufgaben nicht möglich. Die FS konzentriert sich auf die Beantwortung von Anfragen und die Beratung bei Projekten. Kontrollen können wegen mangelnder Kapazitäten keine durchgeführt werden. Die FS prüft aber regelmässig die Protokolle im Zusammenhang mit den Videoüberwachungen der Stadt.

Die Leiterin der FS erfüllt ihre Aufgaben gut. Sie nimmt sie engagiert und motiviert wahr. Bei Aufgaben, bei denen alle Gemeindefachstellen für Datenschutz tangiert sind, übernimmt sie meist eine führende und koordinierende Funktion. Das begrüsst die FDS sehr, dient es doch einer effizienten und qualitativ hochwertigen Aufgabenerfüllung. 30 Stellenprozente erachtet die FDS für die Aufgabenerfüllung als zu wenig. Um den gesetzlichen Auftrag für eine Stadt von der Grösse von St.Gallen erfüllen zu können, sind nach Ansicht der FDS etwa 80 bis 100 Stellenprozente erforderlich. Es ist wichtig, dass Kontrollen durchgeführt werden können. Diese Aufgabe dient nebst der Einhaltung der Datenschutzbestimmungen auch der Sensibilisierung der Stellen. Zudem erhöhen sie bei der FS das Verständnis für die Abläufe und Aufgabenerfüllung der öffentlichen Organe. Die Finanzkontrolle erfüllt ihre Aufgabe unabhängig, das gilt auch für die FS. Dadurch, dass die Leiterin FS aber noch andere Aufgaben bei der Finanzkontrolle übernimmt, entsteht zumindest in zeitlicher Hinsicht eine gewisse Konkurrenz, die zu Lasten der Aufgabenerfüllung beim Datenschutz gehen kann. Die FDS ist der Ansicht, dass mit einer anderen organisatorischen Lösung, beispielsweise der Herauslösung des Datenschutzes aus der Finanzkontrolle, die Unabhängigkeit gestärkt werden kann. Die Anforderungen an die Unabhängigkeit der Datenschutzbehörden sind stetig gestiegen, weshalb darauf ein besonderes Augenmerk gelegt werden muss. Zwar ist zu begrüssen, dass die Zusammenarbeit mit den Informatik-Diensten der Stadt St.Gallen gut funktioniert. Für die Beratung der FS fehlt den Informatik-Diensten aber die Unabhängigkeit.

Zusammenfassend ist die FDS der Ansicht, dass Ressourcen und Anbindung der FS geprüft werden sollten. Sie hat dies der FS und dem Stadtrat so mitgeteilt.

4.2 Erfahrungsaustausch

Am regelmässigen Austausch der FDS mit den Gemeindefachstellen für Datenschutz waren Prüfungen von Privaten, die Gemeindeaufgaben erfüllen Thema, ebenso Pupil (Schuladministrationssoftware der Volksschulen) und Pupil Messenger. Zudem besprachen die Stellen das zukünftige Vorgehen bei Vorabkonsultationen im Bereich e-Government. Dabei sind jeweils sowohl Kanton als auch Gemeinden involviert. Des Weiteren waren die Veröffentlichung von Eigentümerdaten im Geoportal und Datenschutzerklärungen bei öffentlichen Organen Diskussionspunkte.

4.3 Leistungsvereinbarung IT-Audit

Im Berichtsjahr konnte die FDS eine Stelle IT-Audit bei sich besetzen (siehe dazu auch Ziff. 12). Die Gemeindefachstellen für Datenschutz verfügen bisher nicht über derartiges Know-how. Mit zunehmender Digitalisierung ist es aber unerlässlich, entsprechendes und unabhängiges Wissen zu besitzen. Aus diesem Grund schlossen die Gemeindefachstellen für Datenschutz mit der FDS eine Leistungsvereinbarung ab. Diese ermöglicht den Gemeindefachstellen den Beizug der IT-Audit-Fachperson bei der FDS, wenn sie Bedarf danach haben. Die Vereinbarung wurde im Herbst des Berichtsjahres unterzeichnet. Bisher hat eine Gemeindefachstelle für Datenschutz die Leistungen beansprucht.

5 Vorhaben mit hohem Risiko

5.1 Videoüberwachung Amt

Ein Amt setzte punktuell Videoüberwachung ein. Videoüberwachungen stellen potentiell hohe Risiken für die Grundrechte der betroffenen Personen dar. Bei solchen Vorhaben braucht es eine Vorabkonsultation durch die FDS. Zuerst stellte sich das Amt auf den Standpunkt, dass keine Vorabkonsultation nötig sei, weil die Voraussetzungen nicht erfüllt seien[7]. Die FDS war allerdings der Meinung, dass es sich zwar nicht um eine umfangreiche Videoüberwachung handle. Sie finde allerdings teilweise systematisch in einem öffentlich zugänglichen Bereich statt. Zudem verfügt der Kanton St.Gallen derzeit nicht über eine formell-gesetzliche Grundlage, welche die Videoüberwachung kantonaler Organe regelt. Deshalb und nach Rücksprache mit dem Amt hat dieses das Vorhaben dennoch der FDS zur Vorabkonsultation eingereicht.

Die Videoüberwachung beim Amt dient einerseits der Anmeldung von auswärtigen Gästen beim Empfang und anderseits der Sicherheit. Das Amt war in der Vergangenheit mit mehreren Bedrohungssituationen konfrontiert. Bei einer Überwachung handelt es sich um eine Aufzeichnung, deren Bilder während einer kurzen Zeit aufbewahrt werden, bei den anderen um Echtzeitbeobachtung.

Bei der Videoüberwachung handelt es sich um einen schweren Eingriff in die Grundrechte der Betroffenen. Dies gilt insbesondere für die Mitarbeitenden und Besuchenden, die keine Gefahr für die Sicherheit darstellen. Über die Mitarbeitenden könnte bei einer langen Aufbewahrungsdauer ein Bewegungsprofil entstehen. Deshalb muss die Aufbewahrungsdauer kurz sein. Bei den Besuchenden ist ersichtlich, dass sie einen Bezug zum Amt haben. Das kann je nachdem sensibel sein. Das Amt erfüllt allerdings auch Aufgaben, die nicht sensibel sind, womit nicht zwingend auf einen sensiblen Kontext geschlossen werden kann.

Aufgrund der fehlenden formell-gesetzlichen Grundlage – wobei vorliegendenfalls die Aufzeichnung beim Empfang im Fokus stand – ist der Spielraum für eine Videoüberwachung für kantonale öffentliche Organe sehr klein. Voraussetzung ist, dass bereits relevante Vorkommnisse verzeichnet wurden. An die Verhältnismässigkeit der Massnahme muss zudem ein strenger Massstab gelegt werden. Die Überwachung des Verhaltens der Mitarbeitenden am Arbeitsplatz ist nicht zulässig. Die betroffenen Personen müssen informiert und es muss auf die Videoüberwachung hingewiesen werden. Die Aufzeichnungen dürfen nicht länger als 72 Stunden aufbewahrt werden. Ältere allenfalls noch vorhandene Aufzeichnungen müssen unverzüglich vernichtet werden. Bei der Informationssicherheit machte die FDS Empfehlungen zum Zugriff auf die Sicherungskopien, die Protokollierung der Zugriffe, die Funktionen der Videoüberwachung und zu den Passwörtern. Schliesslich muss regelmässig geprüft werden, ob die Videoüberwachung noch notwendig ist. Tritt ein Videoüberwachungsgesetz in Kraft, muss die Zulässigkeit neu überprüft werden.

Das Amt nahm die Empfehlungen an und sie wurden mehrheitlich bereits umgesetzt.

7 Siehe dazu Merkblatt Vorabkonsultation.

5.2 Videoüberwachung Spital

Bei der Videoüberwachung beim Spital handelt es sich um eine Echtzeitbeobachtung, es finden keine Aufzeichnungen statt. Auch eine solche Videoüberwachung muss die Anforderungen an die Einschränkung eines Grundrechts erfüllen: Es muss eine formell-gesetzliche Grundlage vorhanden sein ebenso ein öffentliches Interesse und der Eingriff muss verhältnismässig sein. Zweck der Videoüberwachung ist die sichere medizinische Versorgung, die Sicherheit der Mitarbeitenden, Patientinnen und Patienten sowie der Besuchenden. Weil es bisher, wie bereits oben erwähnt, keine formell-gesetzliche Grundlage gibt, ist Videoüberwachung bei kantonalen Stellen nur in einem sehr eng begrenzten Rahmen zulässig. Sie muss für die gesetzliche Aufgabenerfüllung unentbehrlich sein. Die Abklärungen der FDS haben ergeben, dass die beim Spital vorgesehenen Videoüberwachungen sich darauf stützen können. Der Einsatz muss zudem verhältnismässig sein. Diese Voraussetzung erachtet die FDS in den meisten Fällen als erfüllt. In einem Fall laufen noch Abklärungen. Ausserdem muss ein Videoüberwachungsreglement erstellt werden.

5.3 M365

Auch im Berichtsjahr befasste sich die FDS mit M365. Zwei selbständige öffentliche Stellen planten die Einführung. Bei einer Stelle sollten das Intranet ersetzt und eine einheitliche Datenbasis geschaffen werden. Die andere Stelle beabsichtigte, Teams einzusetzen. Die FDS äusserte sich bereits in ihrem Bericht des Vorjahres[8] im Rahmen des Workplaces 2024 bzw. Drive. Nicht nur der Cloud Act spielt eine Rolle, sondern es muss berücksichtigt werden, dass die USA gemäss Länderliste des EDÖB[9] nicht über ein angemessenes Datenschutzniveau verfügen. Sehr heikel ist zudem die fehlende Kontrolle: Cloud-Lösungen bei einem solch mächtigen international tätigen Unternehmen bedeuten einen grossen Verlust der Kontrolle. Die Verantwortung bleibt aber beim öffentlichen Organ. Das muss diesem bewusst sein. Zudem stellt sich immer wieder die Frage einer Alternative, wenn vertragliche Abmachungen nicht eingehalten werden und das öffentliche Organ gesetzlich verpflichtet ist, die Übertragung rückgängig zu machen.

Eines der Vorhaben wurde sistiert, bis ein konkretes Vorgehen im Bereich der Datenhaltung in der M365-Cloud festgelegt wird. Beim anderen öffentlichen Organ erachtete die FDS die Einsetzung von Teams als datenschutzkonform, weil keine besonders schützenswerten Personendaten damit bearbeitet werden sollen.

8 Siehe Tätigkeitsbericht über das Jahr 2022, Ziff. 5.5.

9 Verordnung über den Datenschutz, SR 235.11, Anhang 1.

5.4 wir.impfen.ch

Im Zusammenhang mit «wir.impfen.ch» waren noch Fragen bei den Aufbewahrungsfristen und der Löschung bzw. Vernichtung offen.[10] Diese konnten geklärt werden. Gestützt auf das Epidemiengesetz werden die Daten während zehn Jahren aufbewahrt. Danach werden sie anonymisiert dem Staatsarchiv übergeben. Die Daten zu den Covid-Zertifikaten werden nach zwei Jahren gelöscht. Die Vernichtung beim Auftragsdatenbearbeiter ist im Auftragsdatenbearbeitungsvertrag geregelt, die Daten werden ein Jahr nach Beendigung des Vertrages vernichtet. Da es sich um sehr sensible Personendaten handelt muss sichergestellt werden, dass sie beim Auftragsdatenbearbeiter vollumfänglich unwiderruflich vernichtet werden. Während der Aufbewahrungsfrist müssen die zum Schutz der Daten notwendigen organisatorischen und technischen Massnahmen umgesetzt werden. So müssen die Daten verschlüsselt aufbewahrt und der Zugriff darauf protokolliert werden. Bei der anonymisierten Ablieferung ans Staatsarchiv muss zudem sichergestellt werden, dass sämtliche Daten auch beim datenbearbeitenden Organ unwiderruflich vernichtet sind.

10 Siehe Tätigkeitsbericht über das Jahr 2022, Ziff. 7.4.

6 Rechtsetzung

6.1 Automatisierte Fahrzeugfahndung

Im Rahmen des revidierten Polizeigesetzes soll auch die automatisierte Fahrzeugfahndung geregelt werden. Die FDS nahm dazu Stellung. Es ist vorgesehen, die Fahrzeuginsassinnen und -insassen bildlich zu erfassen. Darauf sollte zwingend verzichtet werden, auch wenn die Fahrzeuginsassinnen und -insassen sofort verpixelt werden. Damit entsteht bei der Polizei ein sehr umfassendes Bildmaterial, das die ganze Bevölkerung betreffen dürfte. Dabei handelt es sich um eine Datensammlung, die überwiegend unbescholtene Bürgerinnen und Bürger betrifft. Das ist nicht verhältnismässig. Erforderlich sind dafür auch Tools für die Gesichtserkennung. Somit besteht die Gefahr einer totalen Überwachung. Das Bundesgericht hat in einem Entscheid[11] festgehalten, dass «Personenaufnahmen dieses Ausmasses unverhältnismässig wären». Es hielt weiter fest, dass im Polizeirecht das Bestimmtheitserfordernis aufgrund des Regelungsbereichs auf besondere Schwierigkeiten stosse. In einem gewissen Ausmass könne dies jedoch durch verfahrensrechtliche Garantien kompensiert werden und dem Grundsatz der Verhältnismässigkeit komme besondere Bedeutung zu. Wo die Unbestimmtheit von Rechtssätzen zu einem Verlust an Rechtssicherheit führe, müsse die Verhältnismässigkeit umso strenger geprüft werden. Die Verhältnismässigkeit bildet in diesem Fall aber gerade keine Schranke, die sie bei geringerer Bestimmtheit wie im Polizeirecht bilden sollte.

11
BGE 1C_39/2021, Erwägung 4.3.2.

Bei einer Übereinstimmung sollen die Daten 100 Tage aufbewahrt werden. Diese Aufbewahrungsdauer ist lang. Deshalb ist die Umsetzung besonders wichtig. Ist beispielsweise die Fehlerquote hoch, spricht dies eher für eine kürzere Aufbewahrungsdauer. Ansonsten sind zahlreiche Bürgerinnen und Bürger betroffen, bei denen kein konkreter Verdacht besteht.

Zudem ist vorgesehen, dass die FDS periodisch überprüft, ob die rechtlichen Bestimmungen eingehalten werden. Die FDS wehrt sich nicht grundsätzlich dagegen, eine unabhängige Kontrolle ist unverzichtbar. Hinzuweisen ist aber auf die Gefahr, dass die Unabhängigkeit der FDS tangiert wird, wenn der Gesetzgeber für die FDS immer mehr fixe Kontrollen vorsieht. Damit reduziert sich der Spielraum für andere Kontrollen, die aus datenschutzrechtlicher Sicht ebenfalls durchgeführt werden müssen. Es stellt sich auch die Frage der Ressourcen: es können ihr nicht immer mehr Aufgaben überbunden werden, ohne gleichzeitig die Ressourcen zu thematisieren.

6.2 Grundbuchverordnung

Die kantonale Verordnung über das Grundbuch sollte dahingehend geändert werden, als dass die ohne Interessennachweis einsehbaren Daten des Grundbuchs neu verpflichtend für alle Gemeinden flächendeckend elektronisch einsehbar werden. Die FDS hat sich zu dieser Neuerung kritisch geäussert und dabei auf ihre bereits früher gemachten Bedenken verwiesen[12]: Die Öffentlichkeit beim Grundbuchamt ist nicht mit der Publikation im Internet vergleichbar. Eine Internetpublikation ist weltweit abrufbar, auch in Ländern ohne gleichwertigen Datenschutz. Die Daten können nicht mehr gelöscht werden und sind beliebig kopier-, verknüpf-, veränder-, und auswertbar. Die betroffenen Personen haben keinerlei Einwirkungsmöglichkeiten und die Verwendung der Daten entzieht sich vollkommen ihrer Kontrolle. Zu beachten ist auch, dass sowohl Kanton als auch Gemeinden eine besondere Verantwortung im Umgang mit den Daten ihrer Bürgerinnen

12
Siehe Tätigkeitsbericht über das Jahr 2016, Ziff. 2.4.

und Bürger haben, die diese ihnen aufgrund von Gesetzen zwingend zur Verfügung stellen müssen. Eine Datenbearbeitung muss stets einen konkreten Zweck verfolgen. Dieser Zweck war der FDS aufgrund der eingereichten Unterlagen nicht ersichtlich. Der FDS fehlten aber auch Ausführungen zur Verhältnismässigkeit und dem öffentlichen Interesse.

6.3 Strafprozessverordnung

Die kantonale Strafprozessverordnung sollte dahingehend ergänzt werden, als dass die Staatsanwaltschaft dem Departement des Innern die Schlussverfügungen betreffend Konkurs- und Betreibungsdelikten automatisch zustellen könne. Die Information sei u.a. für eine sinnvolle Erfüllung der gesetzlichen Aufgabe wesentlich und die rechtliche Würdigung der Strafbehörden sei für das Konkursamt interessant.

Strafbehörden können andere Behörden informieren, soweit diese zur Erfüllung ihrer gesetzlichen Aufgaben auf die Information angewiesen sind. Mit der Verordnung wäre eine voraussetzungslose Bekanntgabe der Schlussverfügungen möglich. Dies widerspricht dem formellen Gesetz: Die im Gesetz vorgesehene Abwägung der Interessen – einerseits der öffentlichen, anderseits der Persönlichkeitsrechte der Parteien – kann mit einer automatischen Datenbekanntgabe nicht vorgenommen werden. Eine solche Bestimmung steht zudem auch nicht im Einklang mit den Grundsätzen der Verhältnismässigkeit und der Datensparsamkeit. Die FDS erachtete die Bestimmung als nicht vereinbar mit dem Datenschutzgesetz.

6.4 Videoüberwachung

Im Berichtsjahr nahm die FDS zur überarbeiteten gesetzlichen Regelung für eine Videoüberwachung Stellung. Zwar verabschiedete die Regierung den Entwurf nicht. Mit Blick auf eine zukünftige Vorlage erachtet es die FDS allerdings als wichtig aufzuzeigen, was aus datenschutzrechtlicher Sicht beachtet werden sollte. Nachfolgend wird deshalb etwas ausführlicher darauf eingegangen: Die FDS begrüsste, dass neu eine Übersicht der Standorte der überwachten Gebiete vorgesehen ist. Sie regte das in früheren Stellungnahmen an. Ebenso begrüsste sie das Unkenntlichmachen der aufgezeichneten Personen. Sehr wichtig ist, dass keine Gesichtserkennung und damit die Bearbeitung von biometrischen Daten erfolgt, sondern dass dafür eine zusätzliche formell-gesetzliche Grundlage erforderlich sei. Die regelmässige Evaluierung der Wirksamkeit sollte für alle öffentlichen Organe verpflichtend sein und deshalb im Gesetz geregelt werden. Auch bei der Echtzeit-Beobachtung findet eine Datenbearbeitung im Sinn des DSG statt. Im Gegensatz zur Wahrnehmung von blossem Auge werden die Daten in einem System bearbeitet. Es können mehrere Personen gleichzeitig darauf Zugriff haben, zudem kann auch eine Aufzeichnung stattfinden. Nicht zuletzt kann das System unter Umständen gehackt werden. Damit hätten (unbefugte) Drittpersonen Zugriff auf diese Echtzeit-Beobachtung. Das ist mit blossem Auge nicht möglich. Für die FDS stellt eine Echtzeit-Beobachtung deshalb ebenfalls eine Bearbeitung gemäss DSG dar. Nach wie vor als ungenügend erachtete die FDS die Bestimmung zum Zweck. Sie ist zu offen formuliert und erlaubt nicht nur allgemein einen sehr grossen Ermessenspielraum, sondern auch ein ausserordentlich weites Einsatzgebiet: Die gesetzlichen Aufgaben der öffentlichen Organe sind sehr vielfältig und bei all diesen könnten gemäss Wortlaut Videoüberwachungen eingesetzt werden. Das ist nicht verhältnismässig. Die Zweckbestimmung genügt deshalb den da-

tenschutzrechtlichen Anforderungen nicht. Nach Ansicht der FDS muss der Zweck auf die Überwachung zum Schutz von Personen und Sachen vor strafbaren Handlungen bzw. zur Verfolgung derselben eingeschränkt werden. Die Delegation zur Normierung auf Verordnungsstufe ist nur rechtmässig, wenn der Zweck auf formeller Gesetzesstufe genügend eingeschränkt wird. Zudem müssen auch Einsichtnahme und Auswertung, die Art der Videoüberwachung, die räumliche und zeitliche Ausdehnung sowie die Bekannt- und Weitergabe der Aufzeichnungen in den Grundzügen im Gesetz geregelt werden. Videoüberwachung darf nur dort eingesetzt werden, wo sich eine besondere Gefahrenlage ergibt; zum Beispiel bei einem Amt, bei dem bereits mehrmals Vorkommnisse innert kürzerer Zeit stattgefunden haben mit einer Gefahr für die Sicherheit von Mitarbeitenden. Eine rein präventive Überwachung ohne besondere Gefahrenlage ist nicht zulässig. Darauf gilt es in der Praxis ein Augenmerk zu richten.

6.5 Merkblatt KI

Im Zug der aktuellen Entwicklungen bei der generativen Künstlichen Intelligenz (KI) wurde ein Merkblatt für die kantonale Verwaltung erlassen. Für Anwendungen der KI wie ChatGPT wird kein Verbot vorgesehen, sondern auf eine rechtskonforme Handhabung unter Berücksichtigung des Datenschutzes verwiesen. Die FDS begrüsst diese Stossrichtung. KI wird je länger je mehr ein unverzichtbarer Bestandteil des Alltags sein. Es ist wichtig, die Mitarbeitenden auf einen datenschutzkonformen und verantwortungsbewussten Umgang zu sensibilisieren.

6.6 Weitere Stellungnahmen

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

- Verordnung über den Volksschulunterricht
- Verordnung über den elektronischen Verkehr in den Verfahren vor dem Migrationsamt
- Einführungsgesetz zur Bundesgesetzgebung über die Krankenversicherung
- Digitalisierung in der Erwerbsersatzordnung
- Vereinbarung zwischen dem Bund und den Kantonen über die Harmonisierung der Informatik in der Strafjustiz
- Modernisierung der Aufsicht bei der AHV-Gesetzgebung
- Änderung des Militärgesetzes
- Konsultation zum «E-ID Technologie-Entscheid»

7 Anzeigen

Im Berichtsjahr bearbeitete die FDS mehrere Anzeigen. Bei verschiedenen Anzeigen konnte die FDS weder eine Verletzung des Datenschutzes noch der Datensicherheit feststellen, da es sich beispielsweise um widersprüchliche Aussagen oder um ein strafrechtliches Verfahren handelte. In zweiterem Fall wird das DSG nicht angewendet. Bei einer Anzeige wurde beanstandet, dass im Schalterbereich einer Stelle offene Akten herumliegen würden. Abklärungen ergaben aber, dass es sich beim beschriebenen Raum nicht um einen öffentlich zugänglichen Raum bzw. Warteraum handelte.

Eine Anzeige betraf die Sensibilisierung betreffend Cybermobbing in einer Schule. Zwei Mitarbeitende des Jugenddienstes besuchten die betroffene Klasse. Ziel war die Sensibilisierung der Schülerinnen und Schüler. Bei dieser Sensibilisierung wurden Screenshots gezeigt, ohne die Namen abzudecken. Immerhin hat der Jugenddienst die Screenshots für den Unterricht so aufbereitet, dass nicht nachvollzogen werden konnte, von welchen Nutzenden sie stammten. Nicht alle Anwesenden waren aber über die Angelegenheit informiert, entweder weil sie kein Handy besassen, oder weil sie nicht der Chat-Gruppe angehörten. Deshalb war es nicht zulässig, die Personendaten zu zeigen. Gerade in solch heiklen Fällen ist es besonders wichtig, die Frage vorgängig abzuklären, ob es nötig ist, Personendaten zugänglich zu machen und ob dies überhaupt zulässig ist. Das muss in jedem einzelnen Fall geklärt werden. Zu berücksichtigen ist auch, dass die Bearbeitung von Personendaten von Minderjährigen besonders sensibel ist. Die FDS machte entsprechende Empfehlungen, welche die betroffene Stelle akzeptierte.

8 Einzelanfragen und Medien

8.1 Allgemeines

Wie in jedem Jahr bearbeitete die FDS auch im Berichtsjahr zahlreiche Einzelanfragen und Anfragen von Medien. Viele Anfragen gab es zum revidierten Bundesgesetz über den Datenschutz, das am 1. September 2023 in Kraft trat. Die Stellen wollten vor allem wissen, ob und wenn ja inwiefern sie davon betroffen seien. Grundsätzlich gilt für öffentliche Organe des Kantons St.Gallen das DSG. Es gibt Ausnahmen, etwa wenn es im Wettbewerb steht und nicht hoheitlich handelt, was beispielsweise beim Weiterbildungsangebot von Hochschulen der Fall ist. Im Folgenden werden ein paar allgemein interessierende Fälle dargelegt.

8.2 Darmkrebsprogramm

Im Berichtsjahr meldeten sich mehrere Bürgerinnen und Bürger mit der Frage, woher die Verantwortlichen des Darmkrebsprogramms ihre Adresse hätten und ob dies datenschutzrechtlich rechtens sei. Zwischen dem Kanton und der Krebsliga besteht eine Leistungsvereinbarung die sich auf das Gesundheitsgesetz stützt. Die FDS äusserte sich bereits im Jahr 2021 zu diesem Vorhaben und kritisierte, dass die Grundlage, worauf sich dieses Programm stütze, für einen Grundrechtseingriff bzw. die beabsichtigte Datenbekanntgabe zu offen und zu wenig bestimmt formuliert sei. Ihr könne nicht direkt entnommen werden, ob ein Darmkrebsvorsorge-Programm eine Staatsaufgabe im Bereich der Gesundheitsvorsorge darstelle oder nicht. Die FDS regte an, eine gesetzliche Grundlage zu schaffen, welche die Anforderungen an einen verfassungsmässigen Grundrechtseingriff genügt. Das Gesundheitsgesetz wird derzeit revidiert.

8.3 Gesetzliche Grundlage Archivierung Patientendossier

Im Zusammenhang mit der Archivierung von Patientendossiers stellte sich die Frage, ob die Grundlage im Archivgesetz genüge. Die FDS empfahl, den Wortlaut insofern zu präzisieren, als von der Anbietepflicht ans Staatsarchiv auch Personendaten erfasst sind, die einer besonderen Geheimhaltung unterstehen. Dies solle bei der nächsten Revision berücksichtigt werden. Das Bundesgericht beurteilte einen Fall aus dem Kanton Basel-Stadt.[13] Dessen Archivgesetz kennt eine entsprechende Bestimmung, welche das Bundesgericht als hinreichend bestimmt qualifizierte.

13
BGE 2C_1024/2021.

8.4 Datenschutzerklärungen auf Webseiten

Im Berichtsjahr gingen bei der FDS mehrere Anfragen zu Datenschutzerklärungen auf Webseiten ein. Die Frage war jeweils, was in einer solchen stehen müsse, damit sie datenschutzkonform sei. Eine Datenschutzerklärung ist für kantonale öffentliche Organe grundsätzlich nicht nötig. Was erlaubt ist, bestimmen die gesetzlichen Grundlagen. Aber auch der Grundsatz der Verhältnismässigkeit muss beachtet werden. Eine Datenschutzerklärung kann Sinn machen, um Transparenz zu schaffen. So kann auf der Homepage zum Beispiel über den Betrieb und die technische Ausgestaltung bzw. über datenschutzfreundliche Mechanismen oder Verschlüsselung informiert werden. Dementsprechend muss sie aber auch kurzgehalten und in verständlicher Sprache verfasst werden.

Die FDS beantwortete Medienanfragen zu den Themen Videoüberwachung in den Kantonen, Cloud, Polizeigesetz und Ressourcen.

9 Register und Verzeichnis der Bearbeitungstätigkeit



Zum Register der Datensammlungen bearbeitete die FDS einige Anfragen mehr als im Vorjahr. Es macht den Eindruck, dass sich im Vergleich zu den Vorjahren mehr Stellen aktiv mit dem Register auseinandersetzten. Die Mehrheit der Fragen war technischer oder administrativer Art. Ferner wurde angefragt, ob das Register gelöscht werden könne, wenn die darauf basierende Datensammlung nicht mehr geführt werde oder ob Internetseiten ebenfalls aufgeführt werden müssten. Zum Verzeichnis der Bearbeitungstätigkeit stellten sich im Berichtsjahr keine Fragen.

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. Dazu gehört auch die im Jahr 2023 neu geschaffene Stelle 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. Die Datenschutzbeauftragten der Ostschweizer Kantone pflegen zudem eine regelmässige Zusammenarbeit mit Austausch über aktuelle Themen.

Auf politischer Ebene wird eine engere Zusammenarbeit der Datenschutzbehörden der Kantone St.Gallen, Thurgau und beider Appenzell angestrebt. Entsprechende Arbeiten unter Einbezug der Datenschutzbehörden sind in Gang.

Wie jedes Jahr erarbeitete die FDS eine Sequenz für das e-Learning Datenschutz und IT-Sicherheit des Kantons. Thema war das Grundrecht auf Privatsphäre und die informationelle Selbstbestimmung sowie die Voraussetzungen für dessen Einschränkung.

11 Leistungsvereinbarung Bistum St.Gallen

Per 1. Februar 2024 schloss die FDS eine Leistungsvereinbarung über die Gewährleistung der Datenschutzfachstelle mit dem Bistum St.Gallen ab. Die Leistungsvereinbarung ist analog derjenigen mit dem Katholischen Konfessionsteil, welche die FDS im Jahr 2020 abgeschlossen hat. Da zwischen Katholischem Konfessionsteil und Bistum viele Berührungspunkte und entsprechende Datenflüsse bestehen, ist es sehr sinnvoll, für beide Organisationen diese Aufgabe zu übernehmen.

12 Personelles und Ressourcen

Seit April des Berichtsjahres verfügt die FDS über einen Mitarbeiter IT-Audit. Sehr viele Geschäfte der FDS beinhalten Fragen der Informationssicherheit. Zuvor arbeitete die FDS eng mit dem Informationssicherheitsbeauftragten des Dienstes für Informatikplanung (DIP) zusammen. Die Zusammenarbeit war sehr gut, die Mitarbeitenden des DIP verfügen aber nicht über Unabhängigkeit. Die Stellenbesetzung bedeutet deshalb eine wesentliche Stärkung der Unabhängigkeit.

Bereits oben wurde die weiter zunehmende Komplexität der Geschäfte angetönt. So können Prüfungen heute meist nicht mehr in kurzer Zeit abgeschlossen werden, sei es, weil Abhängigkeiten zu anderen Vorhaben bestehen oder weil viele verschiedene Parteien involviert sind. Das ist beispielsweise bei Projekten im Bereich von E-Government der Fall. Zur bisherigen Komplexität kommen neuere Themen wie KI. Bereits jetzt beinhalten Anwendungen Komponenten, nicht immer ist das offensichtlich. Nebst der Komplexität nahm im Berichtsjahr die Anzahl der Geschäftseingänge stark zu. Das ist häufig der Fall, wenn es Änderungen bei Datenschutzerlassen gibt. Im Berichtsjahr trat das eidgenössische Datenschutzgesetz in Kraft. Zunehmende Sensibilisierung führt zudem bei öffentlichen Organen tendenziell zu mehr Geschäftseingängen, bei Bürgerinnen und Bürgern zu häufigeren Anfragen. Die FDS war im Jahr 2023 mehr als gut ausgelastet. Ein Ende dieser Entwicklung vorab bei der Komplexität ist nicht absehbar. Ein Augenmerk wird die FDS auf Aufgaben richten, die der FDS zusätzlich überbunden werden. Die Erfüllung solcher zusätzlicher Aufgaben wird nur möglich sein, wenn auch entsprechende Ressourcen zur Verfügung stehen.

13 Prüfprogramm 2024

Die FDS legt für das Jahr 2024 folgendes Prüfprogramm fest:

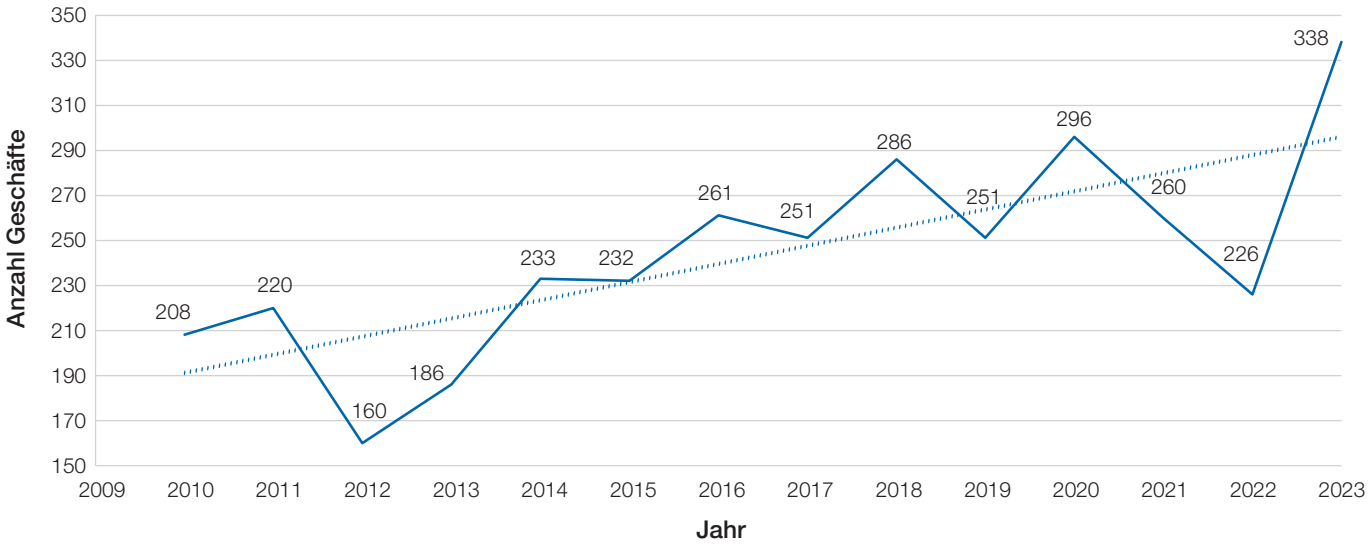
- Plattform Weiterbildungsangebot für Lehrpersonen (aprendo)
- Heimverwaltungslösung Connet
- Schengenkontrolle bei der Kantonspolizei
- Zugriffe auf kantonale Einwohnerdatenplattform
- Arbeitsbesuch bei einer Gemeindefachstelle für Datenschutz

14 Antrag

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

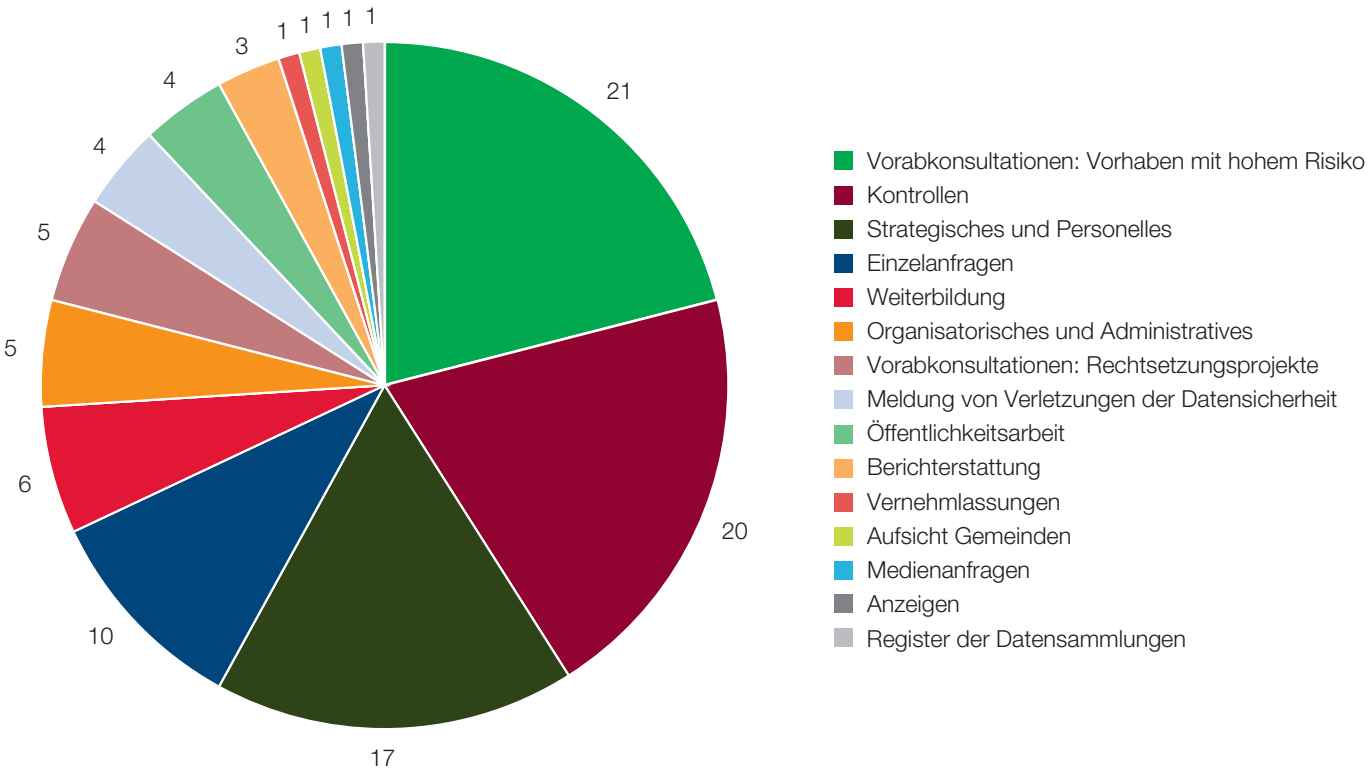
Kantonale Fachstelle für Datenschutz
Corinne Suter Hellstern, Leiterin

Geschäftseingänge[1]



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

Aufgabenverteilung nach Art in Prozent



Kantonsrat des Kantons St.Gallen
Geschäft 32.24.03

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