dsb
datenschutzbeauftragte
des kantons zürich

Tätigkeitsbericht 2025

Vorwort

Die Datenschutzbeauftragte Dr. Dominika Blonski am Jubiläumsanlass. Foto: dsb

Die Datenschutzbeauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht (§ 39 IDG).

Der vorliegende 31. Tätigkeitsbericht deckt den Zeitraum vom 1. Januar 2025 bis und mit 31. Dezember 2025 ab und erscheint ausschliesslich digital mit audiovisuellen Inhalten auf

www.datenschutz.ch/tb *(www.datenschutz.ch/tb)*.

Im Berichtsjahr feierte die Datenschutzbeauftragte das 30-jährige Bestehen der kantonalen Datenschutzgesetzgebung und damit auch ihrer Behörde. Das Gesetz über die Information und den Datenschutz (IDG) ist am 1. Januar 1995 in Kraft getreten. Mit verschiedenen Aktivitäten wie dem Jubiläumsanlass oder dem Tag der offenen Tür hat die Datenschutzbeauftragte Behördenmitgliedern, Verwaltungsmitarbeitenden sowie politischen Vertreterinnen und Vertretern ihr Tätigkeitsgebiet näher bringen können.

Das revidierte Gesetz über die Information und den Datenschutz (IDG) sieht unter anderem neue Aufgaben der Datenschutzbeauftragten in Bezug auf das Öffentlichkeitsprinzip vor.

Im November 2025 hat der Kantonsrat die Detailberatung zur Totalrevision des Gesetzes über die Information und den Datenschutz durchgeführt und dem revidierten Gesetz im März 2026 zugestimmt. Dieses sieht unter anderem neue Aufgaben der Datenschutzbeauftragten in Bezug auf das Öffentlichkeitsprinzip vor.

Aktuelles Thema bleiben Auslagerungen von Datenbearbeitungen. Mehrere öffentliche Organe haben der Datenschutzbeauftragten im Berichtsjahr Auslagerungsprojekte von Softwareanbietern, externen Plattformen oder Cloud-Lösungen vorgelegt. Das IDG hält für die Auslagerung klare Vorgaben fest. Zunehmend setzen öffentliche Organe künstliche Intelligenz (KI) in ihrem Alltag ein. Die datenschutzrechtlichen Bestimmungen schliessen Datenbearbeitungen durch KI-Lösungen ein. Beim Einsatz von KI kann ebenfalls eine Auslagerung vorliegen.

Die Digitalisierung der Verwaltung prägte auch das Jubiläumsjahr

Im Jahr 2025 feierte die Datenschutzbeauftragte sowohl das 30-jährige Bestehen der kantonalen Datenschutzgesetzgebung als auch jenes ihrer Behörde. Das Gesetz über die Information und den Datenschutz (IDG) ist am 1. Januar 1995 in Kraft getreten. 30 Jahre später hat der Kantonsrat eine Totalrevision des IDG vorgenommen. Das Öffentlichkeitsprinzip kommt neu in den Verantwortungsbereich der Datenschutzbeauftragten. Die Datenschutzbeauftragte beschäftigte sich auch im Jubiläumsjahr mit verschiedenen Projekten und Fragen rund um das Thema Digitalisierung bei öffentlichen Organen.

Im Rahmen des Jubiläumsjahres führte die Datenschutzbeauftragte verschiedene Aktivitäten durch. Am Jubiläumsanlass Ende Januar konnte die Datenschutzbeauftragte neben alt Bundesrat Moritz Leuenberger, Kantonsratspräsident Jürg Sulser und Regierungspräsidentin Natalie Rickli alt Regierungsrat Markus Notter sowie den ehemaligen Datenschutzbeauftragten Bruno Baeriswyl begrüssen, die am Podium, mit Referaten und Grussworten zum Gelingen des Anlasses beitrugen. Dr. Anna Jobin, Forscherin und Dozentin an der Universität Freiburg, brachte in ihrem Referat zum Thema «KI: Die neuen Herausforderungen für Politik und Gesellschaft» das Publikum zum Nachdenken. Umrahmt wurde der Anlass von der Stand-up-Comedian Reena Krishnaraja sowie der Moderatorin Elena Wagen. Auch der traditionelle SommerTalk der Datenschutzbeauftragten Anfang Juli stand mit einem unterhaltsamen Datenschutz-Quiz zwischen Dominika Blonski, Datenschutzbeauftragte, und ihrem Amtsvorgänger, Bruno Baeriswyl, im Zeichen des Jubiläums. Im November konnten Besuchende die Büroräumlichkeiten der Datenschutzbeauftragten kennenlernen und ihr Datenschutzwissen im Escape Room oder beim Pub-Quiz unter Beweis stellen. Ziel der Jubiläumsveranstaltungen war es, Verwaltungsmitarbeitenden, Behördenmitgliedern sowie politischen Vertreterinnen und Vertretern einen vertieften Einblick in das umfassende Tätigkeitsgebiet der Datenschutzbeauftragten zu gewähren.

Digitalisierung und Datenschutz sind kein Widerspruch

Als 1995 die Datenschutzgesetzgebung im Kanton Zürich in Kraft trat, steckte das Internet als Massenkommunikationsmittel noch in den Kinderschuhen. Heute gilt es als wichtiger Katalysator der digitalen Revolution. 30 Jahre später sind künstliche Intelligenz (KI), Chatbots und Clouds auch bei öffentlichen Organen im Einsatz. Gleichzeitig sind in dieser Zeit die Ansprüche an den Datenschutz wie auch die Sensibilisierung der Bevölkerung gewachsen. Digitalisierung und Datenschutz sind kein Widerspruch, im Gegenteil: Nur ein datenschutzkonformer Digitalisierungsprozess schafft das Vertrauen der Bevölkerung in die Verwaltung und deren Digitalisierungsvorhaben.

Die Digitalisierung der Verwaltung schreitet weiter voran, mehrere öffentliche Organe haben digitale Projekte bereits lanciert oder sind daran, diese umzusetzen. Die Datenschutzbeauftragte unterstützt die Organisationen bei der datenschutzkonformen Einführung und Umsetzung ihrer Digitalisierungsprojekte. Auslagerungen von Datenbearbeitungen bleiben für öffentliche Organe aktuell. Die Datenschutzbeauftragte hat 2025 mehrere Auslagerungsprojekte von Cloud-Lösungen, externen Plattformen und Softwareanbietern vorgelegt bekommen. Das IDG definiert den ge-

setzlichen Rahmen für die Auslagerung von Datenbearbeitungen. Vermehrt kommt bei öffentlichen Organen die KI zum Einsatz. Datenbearbeitungen durch KI-Lösungen fallen wie alle Datenbearbeitungen unter die datenschutzrechtlichen Bestimmungen des IDG. Bei KI-Lösungen kann es sich um eine Auslagerung handeln, womit insbesondere entsprechende Vorgaben umzusetzen sind.

Vorgehen beim Einsatz von M365 in Gemeinden
(https://www.datenschutz.ch/tb/2025/vorgehen-beim-einsatz-von-m365-in-gemeinden?token=mZdK7TT8JNeqftvAFS5dQTfpjedqR0y6)

Erste Kontrolle einer KI-Applikation *(https://www.datenschutz.ch/tb/2025/erste-kontrolle-einer-ki-applikation?token=mZdK7TT8JNeqftvAFS5dQTfpjedqR0y6)*

Zentraler Telefondienst für Gewaltopfer
(https://www.datenschutz.ch/tb/2025/zentraler-telefondienst-fuer-gewaltopfer?token=mZdK7TT8JNeqftvAFS5dQTfpjedqR0y6)

Webscans für öffentliche Organe

Immer mehr öffentliche Organe setzen Webapplikationen ein – ein Trend der sich weiter verstärken dürfte. In der Umsetzung arbeiten öffentliche Organe regelmässig mit externen Dienstleistenden zusammen. Eine eigene fachliche Sicherheitsbeurteilung kann für das öffentliche Organ eine grosse Herausforderung darstellen. Webapplikationen sind aus Sicherheitsgründen stets auf dem neuesten Stand zu halten. Ein sogenannter Webscan identifiziert veraltete Webapplikationen und offenbart Sicherheitslücken. Die Datenschutzbeauftragte führt bei öffentlichen Organen solche Webscans durch. Eine frühe Erkennung von Risiken erhöht die Sicherheit der Verwaltung und deren digitalen Angebote.

Webscanning *(https://www.datenschutz.ch/tb/2025/webscanning?token=mZdK7TT8JNeqftvAFS5dQTfpjedqR0y6)*

Wie Mitarbeitende Angriffe auf die Datensicherheit verhindern können

Bei Datenschutzverletzungen sind öffentliche Organe verpflichtet, entsprechende Vorfälle umgehend der Datenschutzbeauftragten zu melden. Verschiedene öffentliche Organe sowie deren Dienstleistende wurden im Berichtsjahr Opfer von Angriffen auf die Datensicherheit. Angreifenden geht es dabei oft darum, nach einem Angriff Geld von den Behörden zu erpressen, um beispielsweise eine Veröffentlichung der Daten zu verhindern. Die Datenschutzbeauftragte berät die betroffene Organisation bei der Bewältigung des Vorfalls. Je nach Situation fordert sie die Umsetzung zusätzlicher Massnahmen, um die Informationssicherheit des öffentlichen Organs zu erhöhen und gleichzeitig das Risiko künftiger Angriffe auf die Datensicherheit zu minimieren. Es gilt, sicherheitsrelevante Prozesse im Betriebsalltag einzubauen. Die öffentlichen Organe müssen die Mitarbeitenden entsprechend schulen und sensibilisieren, um mögliche Angriffsgefahren frühzeitig zu erkennen.

Angriffe auf die Datensicherheit *(https://www.datenschutz.ch/tb/2025/angriffe-auf-die-datensicherheit?token=mZdK7TT8JNeqftvAFS5dQTfpjedqR0y6)*

IDG für die Zukunft gerüstet

Der Kantonsrat hat dem neuen IDG im März 2026 zugestimmt. Es berücksichtigt die neuen technologischen Entwicklungen. Gleichzeitig sieht das Gesetz einen erweiterten Aufgabenbereich für die Datenschutzbeauftragte vor: Fragen rund um das Öffentlichkeitsprinzip sowie ein Schlichtungsverfahren bei Zugangsgesuchen sind künftig auch Teil des Aufgabengebietes der Datenschutzbeauftragten.

Totalrevision des Gesetzes über die Information und den Datenschutz
(https://www.datenschutz.ch/tb/2025/totalrevision-des-gesetzes-ueber-die-information-und-den-datenschutz?token=mZdK7TT8JNeqftvAFS5dQTfpjedqR0y6)

Kontrollen erneut erhöht, Massnahmenumsetzung bei sehr hohen 96 Prozent

Kontrollen

Die Kontrolltätigkeit ist für die Datenschutzbeauftragte ein zentraler Entwicklungsschwerpunkt.

Im Berichtsjahr führte die Datenschutzbeauftragte 77 Kontrollen durch. Damit konnte sie ihre Kontrolltätigkeit gegenüber dem Vorjahr nochmals steigern. Neben Datenschutz-Reviews mit Selbstdeklaration bei Gemeinden setzte die Datenschutzbeauftragte einen Schwerpunkt bei Schulen. Auch die Massnahmenumsetzung zur Behebung der nach Datenschutz-Reviews festgestellten Mängeln bei öffentlichen Organen konnte wiederum gesteigert werden. Die prozentuale Umsetzung der Massnahmen liegt bei sehr hohen 96 Prozent.

KEF	2023	2024	2025
70	60	74	77

Anzahl Kontrollen

KEF	2023	2024	2025
80%	89%	93%	96%

Prozentuale Massnahmenumsetzung

Beratung und Vorabkontrollen

Ein weiterer Entwicklungsschwerpunkt zielt auf die effiziente und wirksame Unterstützung der Verwaltung, damit diese ihre Digitalisierungsziele erreichen kann. Sowohl die Beratungstätigkeit der Datenschutzbeauftragten als auch die durchgeführten Vorabkontrollen betrafen wiederum vordergründig komplexe Digitalisierungsprojekte. Gegenüber 2024 blieb die Anzahl der Beratungen im Jahr 2025 etwa gleich.

KEF	2023	2024	2025
900	793	850	851

Anzahl Beratungen

Aus- und Weiterbildung

Auch im aktuellen Berichtsjahr konnte die Datenschutzbeauftragte Referate auf Gemeindestufe und bei Veranstaltungen, insbesondere zu Digitalisierungsthemen

sowie künstlicher Intelligenz (KI), halten. Bei öffentlichen Organen bleibt der Bedarf gross, sich Wissen zu Themen des Datenschutzes und der Informationssicherheit anzueignen. Die Aus- und Weiterbildungstätigkeit der Datenschutzbeauftragten bewegte sich 2025 im durchschnittlichen Rahmen der vergangenen Jahre.

KEF	2023	2024	2025
25	27	45	22

Anzahl Aus- und Weiterbildungen

Websitezugriffe

Die Zugriffe auf die Website www.datenschutz.ch blieben auch im Jubiläumsjahr konstant hoch und erreichten beinahe die Besuche des Vorjahres. Die Website beinhaltet eine umfassende Palette an konkreten Hilfestellungen rund um das Thema Datenschutz und Privatsphäre. Die Datenschutzbeauftragte verweist in den Aus- und Weiterbildungsveranstaltungen und in den Beratungen konsequent auf die Online-Informationen. Die dritte Ausgabe des ausschliesslich digital publizierten Tätigkeitsberichts führte ebenfalls zu zahlreichen Websitebesuchen.

KEF	2023	2024	2025
45 000	74 567	88 360	84 793

Anzahl Websitezugriffe

Totalrevision des Gesetzes über die Information und den Datenschutz

Mit dem Abschluss der Detailberatungen im Kantonsrat am 24. November 2025 hat das Gesetz über die Information und den Datenschutz (IDG) seine neue inhaltliche Gestalt angenommen. Anlässlich der Schlussabstimmung vom 23. März 2026 hat der Kantonsrat dem Erlass in seiner definitiven Fassung zugestimmt. Dem gingen umfangreiche Vorarbeiten und intensive Beratungen voraus. Die Datenschutzbeauftragte hat ihre Position während der mehrjährigen Erarbeitungsphase in verschiedener Form eingebracht.

Das Gesetzgebungsprojekt verfolgte das Ziel, eine übersichtliche und an die digitale Arbeitswelt angepasste Grundlage für den Umgang mit Informationen zu schaffen. Neuen Möglichkeiten zur Aufgabenerfüllung durch die öffentlichen Organe – wie dem Einsatz von algorithmischen Entscheidsystemen – wird mit datenschutzrechtlichen Rahmenbedingungen begegnet. Bedürfnisse der Informationsgesellschaft finden ihren Niederschlag unter anderem in den Bestimmungen zur Nutzbarmachung von maschinenlesbaren Behördendaten (offene Behördendaten).

Neben ihrer Beratungs-, Informations- und Aufsichtsfunktion im Bereich des Datenschutzes kommt der Datenschutzbeauftragten künftig auch eine zentrale Rolle bei der Verwirklichung des Öffentlichkeitsprinzips zu: Die Behörde vereinigt in ihrem Aufgabenbereich neu die Rolle der Datenschutzbeauftragten und der Beauftragten für das Öffentlichkeitsprinzip. Damit folgt der Kanton Zürich der auf Bundesebene und in anderen Kantonen bewährten Praxis, die beiden Funktionen in einer Behörde zusammenzuführen.

Institutionelle Veränderungen bei der Datenschutzbeauftragten

Für die Datenschutzbeauftragte bedeutet das totalrevidierte Gesetz über die Information und den Datenschutz aber zunächst eine grundlegende institutionelle Veränderung. Neben ihrer Beratungs-, Informations- und Aufsichtsfunktion im Bereich des Datenschutzes kommt ihr künftig auch eine zentrale Rolle bei der Verwirklichung des Öffentlichkeitsprinzips zu: Die Behörde vereinigt in ihrem Aufgabenbereich neu die Rolle der Datenschutzbeauftragten und der Beauftragten für das Öffentlichkeitsprinzip. Damit folgt der Kanton Zürich der auf Bundesebene und in anderen Kantonen bewährten Praxis, die beiden Funktionen in einer Behörde zusammenzuführen. Die Datenschutzbeauftragte hat sich bei den Gesetzgebungsarbeiten für diese Lösung stark gemacht und begrüsst es, dass eine Behörde die Rundumsicht für die Bearbeitung von Informationen für sich beanspruchen und entsprechende Synergien nutzen kann. Konkret wird die Beauftragte für das Öffentlichkeitsprinzip ab Inkrafttreten des IDG Schlichtungsverfahren durchführen. Damit kann sie dazu beitragen, dass die öffentlichen Organe Informationszugangsgesuche gemäss einer einheitlichen Praxis behandeln. Gleichzeitig kann die Option eines Schlichtungsverfahrens darauf hinwirken, dass Streitfälle rund um Informationszugangsgesuche aussergerichtlich beurteilt werden.

Auf Antrag des Regierungsrats hat das Kantonsparlament zudem die Anpassung einer weiteren Aufgabe der Datenschutzbeauftragten diskutiert (und schliesslich verworfen), die ebenfalls institutionelle Auswirkungen mit sich gebracht hätte. Es stand zur Debatte, die jährliche Berichterstattung der Datenschutzbeauftragten mit Stellungnahmen derjenigen öffentlichen Organe zu ergänzen, die im Bericht erwähnt werden. Dieses Gegendarstellungsrecht betroffener öffentlicher Organe hätte die Unabhängigkeit der Datenschutzbeauftragten stark beeinträchtigt. Es entspricht einer klaren Lehrmeinung, dass die Unabhängigkeit nur dann gewährleistet ist, wenn die Aufgabenerfüllung alleine bei der Aufsichtsbehörde liegt. Selbst eine potentielle und indirekte Einflussnahme der beaufsichtigten Stellen auf die Aufsichtstätigkeit kann die Unabhängigkeit somit tangieren. Die vorgeschlagene Regelung hätte auch den anwendbaren europarechtlichen Vorgaben widersprochen, welche die Unabhängigkeit von Aufsichtsbehörden im Bereich des Datenschutzes statuieren. Die Datenschutzbeauftragte hat im Verlauf der Debatte ausserdem darauf hingewiesen, dass die öffentlichen Organe während der eigentlichen (zum Zeitpunkt des Tätigkeitsberichts abgeschlossenen) Beratungs- oder Aufsichtstätigkeit ausreichend angehört und miteinbezogen werden. Ein weiterer Einbezug im Rahmen des Tätigkeitsberichts drängt sich auch aus diesem Blickwinkel nicht mehr auf.

Aspekte des totalrevidierten IDG im Bereich des Datenschutzes

Algorithmische Entscheidsysteme

Die neu eingefügten Bestimmungen im IDG zu algorithmischen Entscheidsystemen (AES) führen zu mehr Transparenz des Verwaltungshandelns. Die Datenschutzbeauftragte begrüsst es, dass der Gesetzgeber punktuell spezifische Rahmenbedingungen für den Einsatz der neuen Technologie festgelegt hat. So muss das öffentliche Organ bei der Behandlung von Auskunftsgesuchen ausweisen, ob bei der Bearbeitung der Daten der auskunftssuchenden Person AES verwendet werden. Allgemein werden öffentliche Organe verpflichtet, je ein öffentlich zugängliches Verzeichnis der von ihm verwendeten AES zu führen, sofern sich diese auf die Grundrechte von Personen auswirken können.

Pilotversuche auch für den Einsatz biometrischer Erkennungssysteme im öffentlichen Raum

Ursprünglich sah der Gesetzesentwurf des Regierungsrats vor, dass für biometrische Erkennungssysteme im öffentlichen Raum keine Pilotversuche durchgeführt werden dürfen. Mit dem kategorischen Ausschluss trug er den in der Vernehmlassung generell geäusserten Bedenken gegenüber der Verwendung biometrischer Erkennungssysteme durch öffentliche Organe Rechnung.

Biometrische Erkennungssysteme dienen der Identifikation von Personen aufgrund ihrer körperlichen oder verhaltensspezifischen Merkmale, ein Beispiel dafür ist ein System zur automatischen Gesichtserkennung. Bei einem Einsatz biometrischer Erkennungssysteme werden regelmässig besondere Personendaten bearbeitet.

In Konstellationen, in denen öffentliche Organe zu ihrer gesetzlich verankerten Aufgabenerfüllung künftig besondere Personendaten bearbeiten, die konkrete Bearbeitung aber angesichts komplexer Rahmenbedingungen noch klärungsbedürftig und schwer abschätzbar ist, eröffnen Pilotversuche Möglichkeiten: Bevor die Bearbeitung der besonderen Personendaten langfristig festgelegt und damit zulässig wird, kann

diese testweise und zeitlich begrenzt mit einer Verordnung bewilligt werden. Angesichts der besonderen Gefahr einer Persönlichkeitsverletzung ist das Vorgehen an klar definierte Voraussetzungen und Massnahmen geknüpft.

Der Kantonsrat hat sich gegen einen Ausschluss von Pilotversuchen im Bereich der biometrischen Erkennungssysteme entschieden. Das totalrevidierte IDG sieht damit keine gesonderte Behandlung von biometrischen Erkennungssystemen mit Blick auf Pilotversuche vor; massgebend sind die generell geltenden Bedingungen.

Pilotversuche verfolgen das Ziel einer sachgerechten Regelung: Sie wollen evaluieren, ob die Bearbeitung besonderer Personendaten in der getesteten Art zur Aufgabenerfüllung taugt. Vor diesem Hintergrund hat die Datenschutzbeauftragte zustimmend zur Kenntnis genommen, dass (bei Erfüllen der Voraussetzungen) Pilotversuche auch im Bereich der biometrischen Erkennungssysteme im öffentlichen Raum möglich sein können. Ein Verbot von Pilotversuchen scheint nicht geeignet, der bestehenden Skepsis gegenüber solchen Systemen zu begegnen: Diese dienen gerade als Grundlage für einen fundierten Entscheid, ob und wie eine längerfristige Verankerung in den Rechtsgrundlagen erfolgen soll. Eine sorgfältige und regelkonforme Analyse, ob ein biometrisches Erkennungssystem in die jeweilige Rechtsgrundlage aufzunehmen ist und damit längerfristig zulässig werden soll, ist vor dem Hintergrund der besonderen Gefahr der Grundrechtsverletzung zu begrüssen.

Aspekte des totalrevidierten IDG im Bereich des Öffentlichkeitsprinzips

Ausnahmen vom Informationszugang

Das totalrevidierte IDG nimmt für bestimmte Informationen bereits eine Interessensabwägung vor und klammert diese vom Informationszugang aus. Gemäss dem vom Regierungsrat überwiesenen Entwurf sollten auch die Protokolle nicht öffentlicher Sitzungen in der Verwaltung pauschal von Informationszugangsgesuchen ausgenommen werden. Die Datenschutzbeauftragte und künftige Beauftragte für das Öffentlichkeitsprinzip nahm positiv zur Kenntnis, dass der Kantonsrat diesem Antrag nicht gefolgt ist. Eine derart einschneidende Eingrenzung des Geltungsbereichs wäre mit der insgesamt beabsichtigten Stärkung des Öffentlichkeitsprinzips und dessen institutioneller Verankerung kaum in Einklang zu bringen gewesen.

Aufgaben der Beauftragten im Bereich des Öffentlichkeitsprinzips

Im bei der künftigen Beauftragten für das Öffentlichkeitsprinzip angesiedelten Zuständigkeitsbereich sticht die Durchführung von Schlichtungsverfahren hervor. Daneben nimmt die Beauftragte weitere Aufgaben wahr, die in ihrer Ausprägung und Schwerpunktsetzung nicht vollständig identisch sind mit ihren Aufgaben im Datenschutzbereich.

Analog zum Bereich des Datenschutzes wird sich die Beauftragte gemäss ihrem neuen gesetzlichen Auftrag der Sensibilisierung der Öffentlichkeit für das Öffentlichkeitsprinzip widmen. Zudem wird sie ebenfalls die Rolle einer Anlauf- und Beratungsstelle für Privatpersonen und für öffentliche Organe bei Fragen zum Informationszugang einnehmen. Ihr kommt schliesslich auch die Aufgabe zu, neue Erlasse – nun auch aus der Perspektive des Öffentlichkeitsprinzips – zu beurteilen.

Vorgehen beim Einsatz von M365 in Gemeinden

Verschiedene Gemeinden haben die Datenschutzbeauftragte angefragt, was bei der Einführung von M365-Applikationen zu beachten sei.

Der Einsatz von cloudbasierten M365-Applikationen bei öffentlichen Organen ist nur unter bestimmten Voraussetzungen datenschutzrechtlich zulässig. Gestützt auf US-Gesetze wie den CLOUD Act können amerikanische Behörden Microsoft verpflichten, in der Microsoft Cloud bearbeitete Informationen herauszugeben. Öffentliche Organe dürfen daher sensitive Informationen wie besondere Personendaten und Informationen, die dem Berufsgeheimnis oder einem besonderen Amtsgeheimnis unterstehen, nicht ohne technische Schutzmassnahmen in der Cloud von Microsoft bearbeiten. Andernfalls ist ein hybrider Betrieb zu implementieren, in dem besondere Personendaten und geheimnisgeschützte Informationen nicht in der M365-Cloud-Umgebung bearbeitet und gespeichert werden. Im Leitfaden M365 in Gemeinden sind die Umsetzungsvarianten beschrieben.

Die Datenschutzbeauftragte hat darauf hingewiesen, dass eine Vorabkontrolle bei der Einführung von M365 grundsätzlich nicht notwendig ist, sofern die Gemeinde eine der beschriebenen Varianten umsetzt. Sie hat die Gemeinden angewiesen, die benötigten Unterlagen wie zum Beispiel Datenschutz-Folgenabschätzung (DSFA), Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) und Verträge mit Microsoft selbstständig zu erstellen. Bei Umsetzungsfragen stand sie beratend zur Verfügung.

Zentraler Telefondienst für Gewaltopfer

Die Datenschutzbeauftragte führte beim 2025 in Betrieb genommenen zentralen Telefondienst für Gewaltopfer der Opferberatung Zürich einer Vorabkontrolle durch. Sie legte ihr Hauptaugenmerk dabei auf die Auslagerung von Datenbearbeitungen an externe Dienstleistende. Solche Auslagerungen unterliegen im Bereich des Opferhilfegeheimnisses strengen Voraussetzungen.

Seit dem 1. November 2025 betreibt die Opferberatung Zürich im Auftrag des Kantons einen zentralen 24/7-Telefonberatungsdienst für Gewaltopfer. Dieser Telefondienst nimmt rund um die Uhr Anrufe entgegen und leitet bei Bedarf und mit dem Einverständnis der Anrufenden diese an eine geeignete Opferberatungsstelle im Kanton weiter. Das Angebot stellt einen ersten Schritt auf dem Weg zur schweizweiten Einführung der dreistelligen Notfallnummer für Gewaltopfer (142) dar. Dies ist eine Vorgabe der Istanbul-Konvention, dem Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt.

Die Datenschutzbeauftragte überprüfte den Einsatz des für das Projekt beschafften Systems im Rahmen einer Vorabkontrolle auf seine Konformität mit den Vorgaben des Datenschutzes. Beim beschafften System handelt es sich um eine Clientanwendung, über die aus dem Gebiet des Kantons Zürich eingehende Anrufe entgegengenommen werden können. Eine Applikation Gesprächsleitfaden dient zudem zur Unterstützung der Telefongespräche und zur Weiterleitung an die anerkannten Opferberatungsstellen des Kantons Zürich.

Die Datenschutzbeauftragte hat festgehalten, dass Datenbearbeitungen unter dem Opferhilfegeheimnis nur dann ausgelagert werden dürfen, wenn die geschützten Daten gegenüber dem Dienstleister vollständig verschlüsselt werden. Ebenfalls möglich ist eine Auslagerung, wenn Mitarbeitende des Dienstleisters explizit für die konkrete Datenbearbeitung bestimmt sowie in die funktionale Hierarchie des auslagernden öffentlichen Organs eingebunden und seinem Kontroll- und Weisungsrecht unterstellt werden.

Da im Bereich der Opferberatung mit dem Opferhilfegeheimnis ein besonders strenges Amtsgeheimnis gilt, hat die Datenschutzbeauftragte bei dieser Vorabkontrolle ein spezifisches Augenmerk auf die Auslagerung von Datenbearbeitungen an externe Dienstleistende gelegt. Sie hat festgehalten, dass Datenbearbeitungen unter dem Opferhilfegeheimnis nur dann ausgelagert werden dürfen, wenn die geschützten Daten gegenüber diesen Dienstleistenden vollständig verschlüsselt werden. Ebenfalls möglich ist eine Auslagerung, wenn Mitarbeitende des Dienstleisters explizit für die konkrete Datenbearbeitung bestimmt sowie in die funktionale Hierarchie des auslagernden öffentlichen Organs eingebunden und seinem Kontroll- und Weisungsrecht unterstellt werden. Die so bestimmten Mitarbeitenden haben sich zudem zur Wahrung des Opferhilfegeheimnisses zu verpflichten.

Mit Blick auf die Informationssicherheit sind vom externen Dienstleister zusätzlich Nachweise einzufordern, dass angemessene Massnahmen zum Schutz der Daten vorhanden sind. Dies kann durch den Nachweis einer Zertifizierung oder zusätzliche Evidenzen erfolgen. Dabei sind zum Beispiel folgende Themen zu berücksichtigen: Verwaltung aller Informationssicherheitsmassnahmen im Rahmen eines Informati-

onssicherheits-Managementsystem, Sicherheit der Softwareentwicklung, Sicherheit der Konfiguration sowie Umsetzung des Privacy-by-Designs- und Privacy-by-Default-Prinzips, Verschlüsselung der Datenablage (Datenbank und Speicher) sowie aller externen Verbindungen, Protokollierung und Überwachung, Sicherheit der Patch- und Schwachstellenmanagement-Prozesse, Sicherheit der Authentifizierung und Autorisierung, wirksame Mandantentrennung, Netzwerksicherheit, datenschutzkonforme Nutzung von Drittdiensten sowie Behandlung von Anwendungsrisiken.

Darüber hinaus hat die Datenschutzbeauftragte im Rahmen der Vorabkontrolle darauf hingewiesen, dass durch die Opferberatung Zürich sicherzustellen ist, dass die notwendigen fernmeldedienstrechtlichen Rechtsgrundlagen für den Betrieb der Notrufnummer vorliegen. Für die Aufbewahrung und sichere Löschung aller Daten sind Prozesse zu definieren und zu dokumentieren. Zudem ist sicherzustellen, dass mit den festzulegenden Löschfristen die Rechenschaftsfähigkeit gewährleistet werden kann. Schliesslich hat die Datenschutzbeauftragte festgehalten, dass Betroffene auf Verlangen Zugang zu den sie betreffenden Datenbearbeitungen erhalten und die weiteren Rechte gemäss IDG geltend machen können müssen und entsprechende Prozesse festzulegen sind.

Chat-Beratung bei der Opferberatung Zürich

Die Opferberatung Zürich bietet gemäss Leistungsvereinbarung Beratungsleistungen neu auch via Chatfunktion an. Damit soll das Dienstleistungsangebot mit einem zusätzlichen Kanal zur Kontaktaufnahme niederschwellig zugänglich gemacht werden.

Da die im Chat bearbeiteten Inhalte in aller Regel besonderen Personendaten sind und durch die Schweigepflicht nach Opferhilfegesetz einem besonderen Amtsgeheimnis unterliegen, wurde der zur Realisierung der Chatfunktion beigezogene IT-Anbieter eingehend beurteilt. Die Datenschutzbeauftragte hat im Rahmen ihrer Vorabkontrolle festgehalten, dass die Inhalte der Beratung zur Wahrung des besonderen Amtsgeheimnisses gegenüber dem Anbieter (und den seinerseits beigezogenen Unternehmen) zu verschlüsseln sind. Die Kontrolle über den Schlüssel hat dabei bei der Opferberatung Zürich zu verbleiben. Alternativ kann sie auch je nach Unternehmensstruktur des Anbieters beziehungsweise seiner Unterauftragnehmer eine Einbindung von Mitarbeitenden in das besondere Amtsgeheimnis erwägen.

Verwaltungsweite Druck- und Scan-Infrastruktur mit KI-gestützten Möglichkeiten

Wenn eine Behörde IT-Dienstleistungen zentral bereitstellt, stellt sich die Frage der Abgrenzung von Verantwortlichkeiten zwischen dem Bereitsteller und den nutzenden Stellen. Die Datenschutzbeauftragte hat die Thematik anhand der einheitlichen Druck- und Scan-Infrastruktur in der Verwaltung sowie in Mittel- und Berufsfachschulen aufgenommen und auf massgebende Punkte hin sensibilisiert.

Das Amt für Informatik (AFI) hat der Datenschutzbeauftragten im Jahr 2025 eine zentrale Input- und Output-Management-Lösung vorgestellt. Im Rahmen einer Vorabkontrolle hat sich die Datenschutzbeauftragte mit der Ausgestaltung einer Druck- und Scan-Infrastruktur befasst, die in der gesamten Verwaltung sowie in Mittel- und Berufsfachschulen eingesetzt wird und die bisher dort verwendeten Einzellösungen ablösen soll. Zu deren Realisierung zieht das AFI einen Schweizer Anbieter bei, der die Infrastruktur als cloudbasierte Software as a Service anbietet und in mehreren Schweizer Rechenzentren hostet. Die Lösung bietet neben den Basisfunktionen Drucken und Scannen auch die Möglichkeit, KI-gestützte Funktionen zu nutzen (beispielsweise zur Kategorisierung von Geschäftsfällen und deren direkten Ablage in den jeweiligen Fachapplikationen).

Insgesamt verfolgt das AFI den Ansatz, dass die Anwendung für sämtliche in der Verwaltung und in den Mittel- und Berufsfachschulen anfallenden Dokumente genutzt werden kann. Das bedeutet, dass diese auch besondere Personendaten und geheimnisgeschützte Inhalte in der Druck- und Scan-Infrastruktur bearbeiten. Aufgrund dieses Anspruchs an die Lösung hat die Datenschutzbeauftragte erhöhte Anforderungen an die Auslagerung der Datenbearbeitung an den Anbieter formuliert. Das AFI kommt mit der Bereitstellung der Druck- und Scan-Infrastruktur dem gesetzlichen Auftrag zur Querschnittsdienstleistung im Bereich Informatik nach. Somit liegt es in der Zuständigkeit des AFI, die Lösung dem erhöhten Schutzbedarf entsprechend auszugestalten und dies auch in der Zusammenarbeit und Vertragsausgestaltung mit dem beigezogenen Anbieter sicherzustellen. Konkret hat das AFI mittels technischer Vorkehrungen dafür zu sorgen, dass die in der Infrastruktur bearbeiteten Druck- und Scanaufträge für den Anbieter nicht einsehbar sind. Alternativ kann das AFI auch konkret bezeichnete Mitarbeitende des Anbieters in seine funktionale Hierarchie einbinden und an strafbewehrte Schweigepflichten binden.

Unabhängig davon bleiben aber auch in dieser Konstellation die Verwaltung und die erwähnten Schulen dafür verantwortlich, dass sie die Infrastruktur gemäss den für sie geltenden Vorgaben nutzen.

Unabhängig davon bleiben aber auch in dieser Konstellation die Verwaltung und die erwähnten Schulen dafür verantwortlich, dass sie die Infrastruktur gemäss den für sie geltenden Vorgaben nutzen. Dem AFI als Bereitsteller kommt eine entsprechende Informationspflicht zu. Insbesondere bezüglich der aktivierbaren KI-gestützten Funktionen hat das AFI die nutzenden Behörden dafür zu sensibilisieren.

Darüber hinaus hat die Datenschutzbeauftragte für die Ausgangslage einer zentral bereitgestellten, dezentral genutzten Anwendung auf weitere datenschutzrechtlich relevante Aspekte hingewiesen. So ist etwa vorgängig zu klären, ob das AFI oder die

Verwaltung und die Schulen dafür verantwortlich sind, einen Datenschutzvorfall im Zusammenhang mit der Infrastruktur an die Datenschutzbeauftragte zu melden. Gleiches gilt für die Behandlung von Gesuchen um Zugang zu den eigenen Daten. Da diese auch Daten über den Zugriff auf die eigenen Personendaten umfassen, hat das AFI diese Angaben gegebenenfalls ergänzend für die Gesuchsbeantwortung durch die Verwaltung oder Schulen bereitzustellen.

Neues kantonales Personalmanagement- und Lohnadministrationssystem

Im Rahmen einer Vorabkontrolle hat die Datenschutzbeauftragte das kantonale Grossprojekt eines neuen kantonalen Personalmanagement- und Lohnadministrationssystems geprüft. Dieses umfasst die Ablösung der bisherigen Systeme durch eine cloudbasierte Lösung.

Mit dem neuen System werden Personaldaten von Personalmanagement und Lohnadministration von rund 70'000 Mitarbeitenden der kantonalen Verwaltung künftig in einer Cloud bearbeitet. Davon sind auch besondere Personendaten betroffen. Das zuständige Amt hat die Bearbeitung von Personendaten an ein internationales Unternehmen ausgelagert. Die Datenschutzbeauftragte hielt ihre Prüfungsergebnisse in einem Bericht zuhanden des zuständigen Amtes fest. Zentral ist, dass die Privatsphäre der Staatsangestellten trotz der technologischen Komplexität einer Cloud-Lösung gewahrt bleibt.

Beim Projekt Aurora sind verschiedene Organisationseinheiten der kantonalen Verwaltung involviert: Das Amt für Informatik (AFI) stellt die Technik bereit, das Personalamt definiert die Prozesse und die einzelnen öffentlichen Organe wie Direktionen oder Ämter speisen die Personendaten ihrer Mitarbeitenden ein. In einer solchen Struktur besteht die Gefahr, dass die datenschutzrechtliche Verantwortung in Vergessenheit gerät. Die Datenschutzbeauftragte hielt fest, dass die Rollenverteilung zu Beginn der Prüfung nicht ausreichend klargestellt war: Wer ist zuständig, wenn eine Mitarbeiterin wissen möchte, welche Personendaten über sie gespeichert sind? Wer bearbeitet Gesuche zur Löschung von Personendaten? Die Datenschutzbeauftragte riet zur Erstellung einer Übersichtsdokumentation (zum Beispiel eine Verantwortlichkeitsmatrix). Diese muss unmissverständlich klären, welches öffentliche Organ für welches Datenpaket die rechtliche Verantwortung trägt. Nur so können die Betroffenenrechte (Auskunft, Berichtigung, Löschung) effektiv garantiert werden. Zudem ist zu klären, für welche Datenbearbeitungen die einzelnen HR-Bereiche der verschiedenen öffentlichen Organe zuständig sind und welche Verantwortung das Personalamt konkret trägt.

Zentral ist, dass die Privatsphäre der Staatsangestellten trotz der technologischen Komplexität einer Cloud-Lösung gewahrt bleibt.

Das Gesetz über die Information und den Datenschutz (IDG) folgt dem Prinzip, dass Daten nur so lange aufbewahrt werden dürfen, wie sie für den Zweck der Bearbeitung notwendig sind. Danach müssen sie gelöscht oder dem Staatsarchiv zur Archivierung angeboten werden. In einem komplexen System wie jenem des Projekts Aurora ist die Umsetzung von Löschfristen technisch anspruchsvoll. Die Datenschutzbeauftragte stellte fest, dass die Konzepte für die automatisierte Löschung und die Schnittstellen zum Staatsarchiv noch zu erstellen sind. Das AFI muss sicherstellen, dass das System die gesetzlichen Aufbewahrungspflichten nicht nur passiv abbildet, sondern aktiv die Löschung unterstützt.

Schliesslich stellte sich die Frage, ob das Unternehmen, das im Auftrag des Kantons die Cloud-Lösung entwickelt hat und betreibt, aufgrund seiner internationalen Konzernstruktur dem US-amerikanischen CLOUD Act untersteht. Der CLOUD Act ermöglicht US-Behörden, von privatrechtlichen Unternehmen, die einen relevanten

Bezug zur USA haben, die Herausgabe von Daten zu verlangen, auch wenn diese Daten von Personen ausserhalb der USA, wie beispielsweise der Schweiz, stammen. Dadurch bleiben den betroffenen Personen die Garantien der internationalen Rechtshilfe verwehrt. Folglich ist die Auslagerung der Bearbeitung von Personendaten mit einer erhöhten Gefahr einer Persönlichkeitsverletzung für die betroffenen Personen verbunden, wenn besondere Personendaten bearbeitet werden. Die Datenschutzbeauftragte hat das AFI deshalb angehalten, zu eruieren, ob und inwiefern der CLOUD Act für die Auslagerung an das beauftragte Unternehmen relevant ist.

Versand von Patientendaten an Krankenversicherungen

Die Datenschutzbeauftragte setzte sich im Rahmen einer Vorabkontrolle mit einem System auseinander, das die Übermittlung von Gesundheitsdaten an die Krankenversicherung vereinfachen und standardisieren soll. Im bestehenden System dieser Klinik sollte eine Funktion geschaffen werden, mit deren Hilfe das Personal alle für die Krankenversicherungen relevanten Informationen zusammentragen und an eine Verbindungsstelle weiterleiten kann. Von da aus kann die Klinik die Personendaten direkt an die Krankenversicherungen weitergeben.

Da mit Gesundheitsdaten besondere Personendaten vorliegen, war vor dem Einsatz des Systems eine Vorabkontrolle durchzuführen. Dabei waren insbesondere zwei Punkte von Interesse. Einerseits werden die besonderen Personendaten an die Krankenversicherungen weitergegeben, andererseits wird die Verbindungsstelle von einem privaten Auftragnehmer betrieben, weshalb auch dieser in den Besitz der Personendaten von Patientinnen und Patienten kommt. Die Personendaten sind dabei für den Betreiber der Schnittstelle verschlüsselt, sodass er keinen Einblick hat.

Die Datenschutzbeauftragte überprüfte, ob die Klinik die Personendaten mit den Krankenversicherungen teilen darf. Ebenfalls galt es zu klären, ob und unter welchen Voraussetzungen der Betrieb der Schnittstelle an einen privaten Auftragnehmer ausgelagert werden darf. Da es sich bei den Gesundheitsdaten um besondere Personendaten handelt, dürfen diese nur dann Dritten bekannt gegeben werden, wenn ein Gesetz die Bekanntgabe vorsieht. Für die Krankenversicherungen findet sich die Grundlage im Krankenversicherungsgesetz. Diese dürfen die Gesundheitsdaten bearbeiten, um ihre Aufgaben zu erfüllen, wozu die Überprüfung der Berechnung der Behandlungskosten und der Wirtschaftlichkeit der Behandlungen zählen. Weil die Bekanntgabe mit dem neuen System der gesetzlich vorgesehenen Überprüfung durch die Krankenversicherung dient, dürfen die besonderen Personendaten grundsätzlich mit den Krankenversicherungen geteilt werden. Dabei muss immer auch der Grundsatz der Verhältnismässigkeit beachtet werden. Das Interesse der Krankenversicherung an der Datenbearbeitung muss die Interessen der betroffenen Personen an der Geheimhaltung ihrer Gesundheitsdaten überwiegen. Die Überprüfung der Leistungsansprüche und die Wirtschaftlichkeitskontrolle sind von erheblicher Bedeutung. Es handelt sich um die Durchsetzung volkswirtschaftlicher Interessen und der nachhaltigen Gesundheitsversorgung. Beides dient zudem auch den Bedürfnissen der betroffenen Personen selbst. Dementsprechend erachtete die Datenschutzbeauftragte das Vorhaben der Klinik als verhältnismässig.

Da es sich bei den Gesundheitsdaten um besondere Personendaten handelt, dürfen diese nur dann Dritten bekannt gegeben werden, wenn ein Gesetz eine Bekanntgabe vorsieht. Für die Krankenversicherungen findet sich die Grundlage im Krankenversicherungsgesetz.

Allerdings musste sichergestellt werden, dass nachvollzogen werden kann, wer die Personendaten im System bearbeitet und wie der Zugang gesichert werden kann. Ausserdem hat die Datenschutzbeauftragte auf die Rechte der Patientinnen und Patienten hingewiesen, deren Personendaten bearbeitet werden sollten. Ihnen ist auf entsprechende Anfrage hin Zugang zu den eigenen Personendaten zu gewähren.

Zudem haben sie das Recht, die Personendaten bei Fehlern entsprechend mit Ergänzungen vermerken zu lassen.

Daneben galt es sicherzustellen, dass der Datenschutz auch bei der Schnittstelle, die von einem privaten Auftragnehmer betrieben werden soll, gewahrt wird: Betrifft eine Auslagerung Personendaten, die dem Berufsgeheimnis unterliegen, sind besondere Voraussetzungen zu erfüllen. Zwar können die betroffenen Personen in die Offenbarung von Tatsachen, die dem Berufsgeheimnis unterliegen, einwilligen, sofern die Klinik jedoch als öffentliches Organ tätig ist, darf sie ihre Leistungserbringung nicht an eine solche Einwilligung knüpfen. Sie darf die Datenbearbeitung deshalb nur dann auslagern, wenn die Personendaten so verschlüsselt sind, dass der Auftragnehmer keinen Zugang zum Inhalt hat. Eine solche Verschlüsselung war vorgesehen.

Der Vertrag zwischen der Klinik und dem privaten Auftragnehmer muss ausserdem dem kantonalen Datenschutzrecht Rechnung tragen. Um den Datenschutz sicherzustellen, hat der Regierungsrat die Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen) beschlossen und die ihm unterstellten Verwaltungseinheiten für verbindlich erklärt. Für die Klinik sind diese AGB Auslagerung Informatikleistungen zwar nicht verbindlich, die Datenschutzbeauftragte empfiehlt jedoch, sich an diese zu halten und beriet die Klinik dahingehend. Die Datenschutzbeauftragte brachte deshalb Verbesserungsvorschläge für das ihr vorgelegte Vertragswerk vor, damit der private Auftragnehmer an die einschlägigen datenschutzrechtlichen Pflichten gebunden wird. Der rechtliche Schutz durch das Vertragswerk war aufgrund der Sensitivität der Daten und des damit verbundenen Risikos durch organisatorische Massnahmen zu ergänzen. So sollen beispielsweise nur wenige Mitarbeitende des privaten Anbieters auf die Personendaten von Patientinnen und Patienten zugreifen können. Wo ein Zugriff stattfinden könnte, ist dieser an eine starke Authentifizierung zu knüpfen. Darüber hinaus müssen zusätzliche Gefährdungsanalysen erstellt werden. Es ist sicherzustellen, dass die Klinik ausschliesslich berechtigten Personen physischen Zugang zu den Rechenzentren gewährt. Auch zu diesen organisatorischen Massnahmen hat die Datenschutzbeauftragte die Klinik beraten und Empfehlungen zur Umsetzung mitgegeben.

Anforderungen für den sicheren Versand besonderer Personendaten

Besondere Personendaten dürfen nicht ungeschützt übermittelt werden: Öffentliche Organe sind verpflichtet, beim Versand konsequent auf sichere, verschlüsselte Kommunikationsmittel zu setzen. Weder Bequemlichkeit noch Einwilligungen der betroffenen Personen vermögen fehlende Datensicherheit zu rechtfertigen.

Die Bearbeitung besonderer Personendaten stellt erhöhte Anforderungen an den Datenschutz. Öffentliche Organe sind verpflichtet, durch angemessene technische und organisatorische Massnahmen sicherzustellen, dass diese Daten vor unbefugtem Zugriff geschützt sind.

Ein zentraler Aspekt der Datensicherheit ist der Versand von Personendaten. Während bei Personendaten je nach Kontext ein gewisses Restrisiko hingenommen werden kann, gilt dies für besondere Personendaten nicht. Aufgrund ihres erhöhten Schutzbedarfs müssen sie beim Versand wirksam gesichert werden. Dies bedeutet in der Praxis, dass eine Verschlüsselung zwingend erforderlich ist.

Verschlüsselung als Mindeststandard

Der Versand besonderer Personendaten über unverschlüsselte Kanäle – etwa per E-Mail – genügt den gesetzlichen Anforderungen nicht. Öffentliche Organe haben sicherzustellen, dass geeignete Verschlüsselungstechnologien eingesetzt werden. Dabei stehen verschiedene Möglichkeiten zur Verfügung: Neben klassisch verschlüsselten E-Mails existieren heute auch spezialisierte Plattformen, sichere Webportale oder Messenger-Dienste mit Ende-zu-Ende-Verschlüsselung, die einen datenschutzkonformen Versand ermöglichen.

Die Wahl des konkreten Mittels ist den öffentlichen Organen überlassen, sofern die eingesetzte Lösung dem Stand der Technik entspricht und ein angemessenes Schutzniveau gewährleistet. Entscheidend ist nicht das konkrete Instrument, sondern das Ergebnis: Der Schutz der Vertraulichkeit während der Übermittlung.

Die Einhaltung der Datensicherheitsanforderungen ist für öffentliche Organe eine gesetzliche Pflicht. Eine Einwilligung, die den Verzicht auf angemessene Sicherheitsmassnahmen zum Gegenstand hat, ist rechtlich nicht gültig.

Verantwortung der öffentlichen Organe

Die Verantwortung für die Einhaltung dieser Anforderungen liegt ausschliesslich bei den öffentlichen Organen. Sie haben ihre Prozesse so auszugestalten, dass ein sicherer Versand jederzeit gewährleistet ist. Dazu gehört auch, Mitarbeitende entsprechend zu instruieren und geeignete technische Lösungen bereitzustellen.

Es genügt nicht, die Verantwortung auf betroffene Personen abzuwälzen oder auf deren Verhalten zu vertrauen. Insbesondere ist es unzulässig, den Versand über unsichere Kanäle aus praktischen Gründen zu tolerieren.

Gesetzliche Pflicht

In der Praxis wird bisweilen argumentiert, betroffene Personen hätten in den unverschlüsselten Versand eingewilligt. Die Einhaltung der Datensicherheitsanforderungen ist für öffentliche Organe eine gesetzliche Pflicht. Eine Einwilligung, die den Verzicht auf angemessene Sicherheitsmassnahmen zum Gegenstand hat, ist rechtlich nicht gültig.

Fazit

Der Versand besonderer Personendaten erfordert zwingend den Einsatz geeigneter Verschlüsselungstechnologien. Öffentliche Organe müssen die dafür notwendigen Mittel bereitstellen und deren Anwendung sicherstellen. Alternative Kommunikationsmittel können eingesetzt werden, sofern sie ein angemessenes Schutzniveau bieten. Eine Einwilligung der betroffenen Person vermag fehlende Sicherheitsmassnahmen nicht zu ersetzen. Die Verantwortung für einen rechtmässigen und sicheren Umgang mit Personendaten bleibt in jedem Fall bei den öffentlichen Organen.

Nationales Electronic-Monitoring-System im Kanton Zürich eingeführt

Im Jahr 2025 löste ein von 22 Schweizer Kantonen gemeinschaftlich beschafftes, einheitliches Electronic-Monitoring-System die bestehende Lösung für alle Formen von Electronic Monitoring im Kanton Zürich ab. Die Datenschutzbeauftragte führte eine Vorabkontrolle des Zürcher Anschlusses an das neue Electronic-Monitoring-System durch und machte verschiedene Hinweise zur datenschutzkonformen Umsetzung des Projekts.

Seit 2018 sind alle Kantone verpflichtet, Electronic Monitoring – die elektronische Überwachung des Aufenthaltsortes von Personen als alternative Straf- und Massnahmenvollzugsform – anzubieten. 2019 gründeten 22 Schweizer Kantone, darunter Zürich, einen Verein, der die technischen Einrichtungen für ein gemeinsames, einheitliches Electronic-Monitoring-System beschaffen und betreiben sollte. Im Jahr 2023 beschaffte dieser Verein ein Electronic-Monitoring-System eines britischen Anbieters. Dieses nationale Electronic-Monitoring-System wird vollständig in den Rechenzentren des Kantons Jura gehostet. Es löste 2025 die bisher im Kanton Zürich im Einsatz stehende Lösung für alle Anwendungsformen ab.

Im Rahmen dieser Vorabkontrolle wies die Datenschutzbeauftragte darauf hin, dass es zweifelhaft erscheine, ob eine genügende formell-gesetzliche Rechtsgrundlage für den Einsatz technischer Überwachungsgeräte bestehe, die den Aufenthaltsort des Opfers aufzeichnen und mit dem der zu überwachenden Person abgleichen. Die Rechtsgrundlagen des Electronic Monitoring ermächtigen ihrem Wortlaut nach regelmässig nur zur Überwachung des Täters eines Delikts und nicht auch des Opfers. Sie regte eine Überprüfung an. Ebenfalls überprüfte die Datenschutzbeauftragte, ob die im Rahmen des verwendeteten Systems eingesetzte Authentifizierung des Trägers bei gewissen Feldgeräten über den Fingerabdruck auf einer genügenden Rechtsgrundlage erfolgte.

Da die im Rahmen eines Electronic-Monitoring-Systems zu bearbeitenden Daten regelmässig besondere Personendaten darstellen, hat die Datenschutzbeauftragte auf die nötigen technischen und organisatorischen Massnahmen zum Schutz der Daten hingewiesen.

Im Sinne des Verhältnismässigkeitsgrundsatzes hielt die Datenschutzbeauftragte fest, dass es im Rahmen des Electronic-Monitoring-Systems ausschliesslich dann zu einer Erfassung von Überwachungsdaten kommen darf, wenn eine Auflage für die überwachte Person besteht. Der vom System vorgesehene Einsatz von Google Maps war im Sinne des Verhältnismässikgkeitsgrundsatzes zu überprüfen. Sie wies überdies darauf hin, dass ein manuelles Löschprotokoll für das System zu erstellen und dessen Ausführung zu überprüfen sei.

Da die im Rahmen eines Electronic-Monitoring-Systems zu bearbeitenden Daten regelmässig besondere Personendaten darstellen, hat die Datenschutzbeauftragte auf die nötigen technischen und organisatorischen Massnahmen zum Schutz der Daten hingewiesen. Dazu gehören die Erstellung eines umfassenden Rollen- und Berechtigungskonzeptes mit den entsprechenden Prozessen und einer Zugriffsmatrix, die Zutrittsprotokollierung zum Rechenzentrum und deren regelmässige sowie risikobasierte Kontrolle, die Verwaltung der Sicherheitsmassnahmen in einem zerti-

fizierten Sicherheitsrahmen, beispielsweise nach ISO-Zertifizierung, die Erstellung eines Notfallkonzepts sowie die Dokumentation der Ausserbetriebnahme und Liquidation der Systeme.

Nutzung von MS Teams beim Online-Polizeiposten

Die Datenschutzbeauftragte führte im Jahr 2025 beim Projekt Online-Polizeiposten der Kantonspolizei Zürich (Kapo) eine Vorabkontrolle durch. Mit der eingeschränkten Nutzung der Videotelefonie-App MS Teams und weiteren technischen und organisatorischen Massnahmen liegen angemessene Massnahmen zum Schutz der Vertraulichkeit der im Rahmen des Online-Polizeipostens bearbeiteten Daten vor.

Die Datenschutzbeauftragte führte im Jahr 2025 beim laufenden Projekt Online-Polizeiposten der Kapo eine Vorabkontrolle durch. Im Rahmen dieses Projekts bündelte, ergänzte und richtete die Kapo die Arten der digitalen Anzeigeerstattung und Auskunftserteilung durch die Kapo neu aus. Der Online-Polizeiposten ermöglicht es, mittels Videokonferenz mit einer Polizistin oder einem Polizisten gewisse Deliktarten wie einfache Diebstähle, Cyberdelikte, Sexualdelikte und Telefonbetrug anzuzeigen. Technisch handelt es sich beim Online-Polizeiposten um verschiedene miteinander agierende Einzelkomponenten. Die zentralen Elemente sind dabei die Cloud-Lösungen für Terminvereinbarungen sowie für Videotelefonie.

Die Datenschutzbeauftragte beurteilte den Online-Polizeiposten als geeignetes Instrument für die Terminvereinbarung und Videotelefonie mit der Kapo zur digitalisierten Anzeige von Straftaten sowie zur Auskunftserteilung. Im Sinne des Verhältnismässigkeitsgrundsatzes hielt sie fest, dass durch Prozesse und Kontrollen sicherzustellen ist, dass ausschliesslich die für die genannten Zwecke notwendigen Datenbearbeitungen durchgeführt werden. Ebenso wies sie darauf hin, dass Prozesse für die Aufbewahrung und sichere Löschung der anfallenden Daten, für den Zugang der betroffenen Personen zu den sie betreffenden Datenbearbeitungen sowie für die weiteren Rechte gemäss IDG zu definieren sind.

Im Sinne des Verhältnismässigkeitsgrundsatzes hielt die Datenschutzbeauftragte fest, dass durch Prozesse und Kontrollen sicherzustellen ist, dass ausschliesslich die für die genannten Zwecke notwendigen Datenbearbeitungen durchgeführt werden.

Da im Rahmen der Anzeigen und Auskunftserteilung über den Online-Polizeiposten regelmässig besondere Personendaten bearbeitet werden und für die Videotelefonie die Applikation MS Teams verwendet wird, richtete die Datenschutzbeauftragte ein besonderes Augenmerk auf die Auslagerungskonstellation. Als US-amerikanisches Unternehmen unterliegt Microsoft als Anbieter von MS Teams dem CLOUD Act. Der CLOUD Act ist ein Gesetz der USA und ermöglicht bestimmten US-Behörden, amerikanische Unternehmen zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Im Kontext des CLOUD Act sind daher für besondere Personendaten effektive Massnahmen zu ergreifen, die eine mögliche Kenntnisnahme durch US-Behörden ausschliessen. Dies können technische Lösungen wie eine Verschlüsselung mit Schlüsselmanagement bei der Kapo, eine Anonymisierung oder eine Pseudonymisierung der Daten sein. Die Kapo wählte dabei eine lediglich eingeschränkte Nutzung von MS Teams und deaktivierte die Funktionen für Aufzeichnung, Chat und Dokumentenaustausch. Damit sollte vermieden werden, dass Microsoft Zugriff auf besondere Personendaten erhält.

Schliesslich wies die Datenschutzbeauftragte darauf hin, dass allen Verträgen mit externen Dienstleistenden die AGB des Regierungsrates über die Auslagerung von Informatikleistungen zugrunde gelegt werden müssen. Damit und dank weiterer technischer und organisatorischer Massnahmen liegen angemessene Massnahmen zum Schutz der Vertraulichkeit der im Rahmen des Online-Polizeipostens bearbeiteten Daten vor.

Projekt Datentransportsystem

Die Datenschutzbeauftragte hat bei einem Projekt Datentransportsystem eine Vorabkontrolle durchgeführt. Sie hat sich zu den datenschutzrechtlichen Verantwortlichkeiten geäussert und verschiedene Hinweise zu technischen und organisatorischen Schutzmassnahmen gegeben.

Die betreffende Fachstelle betreibt für die kantonale Verwaltung den institutionalisierten und individuellen Austausch von elektronischen Daten zwischen kantonalen Stellen, Gemeinden und weiteren, auch externen, Stellen. Die Benutzenden können dabei Daten automatisiert zwischen Fachstellen beziehungsweise Fachapplikationen austauschen. Für diesen Datenaustausch bestand seit mehr als zehn Jahren eine Software-Applikation als Datenaustauschplattform. Im Rahmen des Projekts Datentransportsystem wurde dieses ersetzt.

Das System Datentransportsystem besteht aus einem Software Client, der in der Infrastruktur der Benutzenden installiert und betrieben wird, und einer Serverapplikation für die Datenlogistik. Der Software Client prüft in einem Abstand von wenigen Minuten, ob Dateien zum Versand bereitstehen, und verschickt diese über das neue Datentransportsystem an den Empfangsclient. Dieser prüft ebenfalls, ob Dateien auf dem Server des Datentransportsystems zum Download bereitstehen. Die heruntergeladenen Dateien stellt er in einem zu definierenden Ordner einer Fachapplikation oder einer Fachperson zur Weiterverarbeitung zur Verfügung.

Soweit die Fachstelle das Datentransportsystem anderen öffentlichen Organen der kantonalen Verwaltung zur Verfügung stellt, erbringt sie diese Dienstleistung – gestützt auf die Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung sowie die Verordnung über das Gebäude- und Wohnungsregister und die Datenlogistik – in eigener Verantwortung. Wenn das Datentransportsystem jedoch anderen öffentlichen Organen wie Gemeinden oder Dritten zur Verfügung gestellt wird, ist von einer Auslagerung im Sinne des IDG auszugehen.

Die Datenschutzbeauftragte hatte im Rahmen der Vorabkontrolle das Verhältnis zwischen der Fachstelle als Dienstleistungserbringerin und den Benutzenden zu beurteilen: Soweit die Fachstelle das Datentransportsystem anderen öffentlichen Organen der kantonalen Verwaltung zur Verfügung stellt, erbringt sie diese Dienstleistung – gestützt auf die Verordnung über die Organisation des Regierungsrates und der kantonalen Verwaltung sowie die Verordnung über das Gebäude- und Wohnungsregister und die Datenlogistik – in eigener Verantwortung. Wenn das Datentransportsystem jedoch anderen öffentlichen Organen wie Gemeinden oder Dritten zur Verfügung gestellt wird, ist von einer Auslagerung im Sinne des IDG auszugehen. Die Benutzenden bleiben für die Datenbearbeitungen verantwortlich. Soweit es sich um öffentliche Organe handelt, sind die Vorgaben des kantonalen Datenschutzrechts für Auslagerungen zu beachten.

Die Datenschutzbeauftragte hat zudem auf die Notwendigkeit der Umsetzung einer Reihe technischer und organisatorischer Massnahmen hingewiesen. Dazu gehören angemessene Massnahmen gegen physische Bedrohungen (Brand, Wasser, Einbruch etc.), Zutrittskontrollen im Rechenzentrum, die Protokollierung und Überwachung der Zutritte, die Authentifizierung von Administratorinnen und Administrato-

ren an der Webanwendung durch starke Authentisierung, kryptographische Verfahren nach dem aktuellen Stand und deren Dokumentation in einem Kryptokonzept sowie eine sichere Konfigurierung der IKT (Hardening). Härtungsmassnahmen sollten auf einem anerkannten Standard beruhen, wie beispielsweise demjenigen des Center for Internet Security (CIS). Die Konfigurationen sind wo möglich zu überwachen, um Manipulationen zu erkennen.

Elektronische Meldungen zu übertragbaren Infektionskrankheiten

Das Amt für Gesundheit führt eine neue Plattform ein, die es den Laboratorien sowie den behandelnden Ärztinnen und Ärzten erlaubt, eine elektronische Meldung zu übertragbaren Infektionskrankheiten einzugeben und die dafür notwendigen Personendaten an die zuständigen Bundesbehörden zu übermitteln. Die Datenschutzbeauftragte prüfte das Projekt im Rahmen einer Vorabkontrolle.

Auf dieser Plattform werden Gesundheitsdaten bearbeitet. Diese gehören zu den besonderen Personendaten im Sinne des Gesetzes über die Information und den Datenschutz (IDG), bei denen von einem erhöhten Risiko für die Grundrechte der Betroffenen auszugehen ist. Ausserdem läuft die Plattform in der Cloud eines privaten Auftragnehmers. Die Bearbeitung von besonderen Personendaten in der Cloud kann erhöhte Risiken in Bezug auf den Persönlichkeitsschutz von betroffenen Personen mit sich bringen. Deshalb führte die Datenschutzbeauftragte vor dem Einsatz dieser Lösung eine Vorabkontrolle durch. Im Rahmen der Vorabkontrolle prüfte die Datenschutzbeauftragte, ob die Voraussetzungen der geplanten Datenbearbeitung erfüllt sind.

Bezüglich der Rechtmässigkeit der Datenbearbeitung hielt die Datenschutzbeauftragte fest, dass besondere Personendaten wie Gesundheitsdaten nur bearbeitet werden dürfen, wenn dies in einer gesetzlichen Grundlage vorgesehen ist. Entsprechende rechtliche Grundlagen für die Bearbeitung von Gesundheitsdaten finden sich im Zusammenhang mit der Bekämpfung von übertragbaren Krankheiten auf Bundesebene im Epidemiengesetz und auf kantonaler Ebene in der Vollzugsverordnung zur eidgenössischen Epidemiengesetzgebung. Personendaten dürfen ausserdem nur zu dem Zweck bearbeitet werden, für den sie erhoben wurden. Auch diese Voraussetzung war vorliegend erfüllt, denn die Gesundheitsdaten werden für die Überwachung und Früherkennung von übertragbaren Krankheiten erhoben. Die Plattform soll genau diese Früherkennung durch eine Standardisierung vereinfachen.

Das Datenschutzrecht verlangt weiter, dass jede Datenbearbeitung zur Erfüllung der gesetzlichen Aufgaben geeignet und erforderlich ist und die Bearbeitung den Betroffenen vor dem Hintergrund der öffentlichen Interessen zugemutet werden kann. Nur dann ist eine Bearbeitung verhältnismässig. Die neue Plattform ist geeignet, um die öffentliche Gesundheit zu schützen. Zum Schutz der öffentlichen Gesundheit gehört auch die Früherkennung von gefährlichen Krankheiten sowie die damit verbundene Prävention. Durch die Formalisierung des Meldeprozesses wird zudem die Effizienz der Aufgabenerfüllung gesteigert und Fehler bei manuellen Datenbearbeitungsschritten werden vermieden. Eine weniger eingreifende Massnahme, die gleich gut geeignet ist, wurde der Datenschutzbeauftragten nicht vorgelegt.

Mit der Bearbeitung von Gesundheitsdaten geht ein erhebliches Risiko für die Privatsphäre der betroffenen Personen einher. Deshalb ist diese nur dann zumutbar, wenn der Einsatz der neuen Bearbeitung gewichtigen öffentlichen Interessen dient und zum Schutz der besonderen Personendaten entsprechend technische und organisatorische Massnahmen getroffen werden. Der Schutz der öffentlichen Gesundheit vor Infektionskrankheiten dient einem gewichtigen öffentlichen Interesse. Das öffentliche Interesse überwiegt in diesem Fall die privaten Interessen der betroffenen Personen, weshalb die Datenbearbeitung zumutbar ist, sofern auch dem Risiko

angemessene technische und organisatorische Massnahmen durch den Kantonsärztlichen Dienst getroffen werden.

Zum Schutz der öffentlichen Gesundheit gehört auch die Früherkennung von gefährlichen Krankheiten sowie die damit verbundene Prävention. Die Datenschutzbeauftragte prüfte im Rahmen einer Vorabkontrolle, inwiefern der Datenschutz dabei eingehalten wird.

Das IDG sieht vor, dass die Nachvollziehbarkeit der Bearbeitung gewährleistet sein muss. Bei der Bearbeitung von Personendaten auf dieser Plattform werden dazu sämtliche Veränderungen, Zugriffe, Zugriffsversuche und Fehlermeldungen aufgezeichnet. Dadurch kann jederzeit nachvollzogen werden, wie die Personendaten bearbeitet werden. Ausserdem müssen die betroffenen Personen stets Zugang zu den eigenen Personendaten haben. Bei der Plattform fehlte dazu ein Konzept und die Bezeichnung einer zuständigen Stelle. Die Datenschutzbeauftragte wies deshalb darauf hin, dass ein entsprechendes Konzept erarbeitet werden muss, bevor mit dem Einsatz begonnen wird. Die Datenschutzbeauftragte beriet dahingehend, dass sowohl die Nachvollziehbarkeit als auch der Ablauf für Zugangsgesuche berücksichtigt werden muss und entsprechende Prozesse zu erstellen sind.

Da die Plattform in der Cloud eines externen Auftragnehmers läuft, lag ausserdem ein Bearbeiten im Auftrag beziehungsweise eine Auftragsdatenbearbeitung vor. Für Auslagerungen hat der Regierungsrat die allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikdienstleistungen beschlossen und für die zentrale Verwaltung für verbindlich erklärt. Die AGB setzen das IDG in Vertragsbestimmungen um und legen die Mindeststandards des Datenschutzes fest. Die Datenschutzbeauftragte wies deshalb auf die Pflicht hin, die AGB in das Vertragsverhältnis mit dem externen Auftragnehmer zu integrieren. Den Mindeststandards ist in der Vertragshierarchie der höchste Rang zu geben. Sie dürfen weder durch den Hauptvertrag noch durch andere Vertragsdokumente aufgeweicht werden. Weiter ist der Auftragnehmer, der die Cloud betreibt, einer Geheimhaltungs- und Schweigepflicht zu unterstellen. Die Datenschutzbeauftragte wies daraufhin, dass der Vertrag zur neuen Plattform entsprechend angepasst werden muss.

Die AGB des Regierungsrats sorgten im konkreten Fall für die Bereinigung diverser Lücken: Bei der Nutzung einer Cloud ist zum Beispiel erforderlich, dass der Auftragnehmer, der die Cloud betreibt, das öffentliche Organ über die verwendete Technik und die möglichen Orte einer Datenbearbeitung informiert. Sämtliche besonderen Personendaten müssen umfassend verschlüsselt sein. Ausserdem muss der Anbieter die Verschlüsselung während des gesamten Bearbeitungsprozesses inklusive Vernichtung garantieren. Diese Bestimmungen fehlten im ursprünglichen Vertrag. Dieser sah zudem vor, dass der Anbieter bei einer eventuellen Vertragsauflösung für Unterstützungshandlungen entschädigt werden sollte. Auch hier stellte die Datenschutzbeauftragte einen Widerspruch gegen die Mindeststandards der AGB fest, da die Unterstützungshandlungen danach unentgeltlich zu erbringen sind.

Zusätzlich zu diesem rechtlichen Schutz überprüfte die Datenschutzbeauftragte auch die technischen und organisatorischen Massnahmen, die den Datenschutz ergänzend sicherstellen sollen. Dazu gehörte beispielsweise eine klare Definition der Personendaten, die mit den Bundesbehörden ausgetauscht werden, die Beschränkung der zugriffsberechtigten Personen auf die notwendigen Personenkreise und das Erstellen von Gruppen mit verschiedenen Zugriffsberechtigungen. Es müssen Gefährdungsanalysen und umfassende Sicherheitsprüfungen durchgeführt sowie entsprechende Konzepte erstellt werden.

Projekt Digitalisierung Haftaktenprozess

Die Kantonspolizei Zürich (Kapo) digitalisierte im Rahmen des Projekts Digitalisierung Haftaktenprozess ihre Prozesse im Zusammenhang mit der vorläufigen Festnahme von Personen. Die Datenschutzbeauftragte führte einer Vorabkontrolle durch.

Im Rahmen des Projekts Digitalisierung Haftaktenprozess digitalisierte die Kapo ihre Prozesse im Zusammenhang mit der vorläufigen Festnahme von Personen. Um das bestehende Aufnahmeverwaltungssystem abzulösen, wurde dafür die Webapplikation Gefangeneninformations- und Fristensystem (GIFS) entwickelt. Bei der Verhaftung einer Person durch die Kapo werden die Daten des Häftlings im Polizei-Informationssystem POLIS aufgenommen und der Verhaftsrapport sowie weitere Haftakten erstellt. Während diese Daten im Aufnahmeverwaltungssystem der Kapo bisher zusätzlich manuell erfasst wurden, werden die relevanten Daten mit der neuen Systemlösung GIFS über eine Schnittstelle aus dem Polizei-Informationssystem POLIS übernommen. Die anschliessende Administration der Haftfälle, vom Eingang des Häftlings bei der Gefangenenannahme im Polizei- und Justizzentrum Zürich (PJZ) bis zur Entlassung oder Überführung in die Untersuchungshaft, erfolgt in der neuen Applikation. Diese beinhaltet insbesondere auch die Kontrolle der gesetzlich vorgegebenen Fristen für die vorläufige Festnahme, die Erstellung von Verfügungen, die nachvollziehbare Dokumentation von Massnahmen und interner Workflows sowie die Erstellung von Statistiken.

Verschiedene Behörden wie die Staats- und Jugendstaatsanwaltschaften oder das Forensische Institut Zürich sollen direkten Zugriff auf die Applikation GIFS erhalten. Im Rahmen der durchgeführten Vorabkontrolle hat die Datenschutzbeauftragte festgestellt, dass für den vorgesehenen direkten Behördenzugriff jeweils eine formell-gesetzliche Grundlage bestehen muss. Eine solche ist jedoch nicht für alle vorgesehenen Behörden unmittelbar ersichtlich. Sie riet zur genauen Überprüfung der vorgesehenen Zugriffsrechte.

Betroffene müssen auf Verlangen Zugang zu den sie betreffenden Datenbearbeitungen erhalten und die weiteren Rechte gemäss IDG geltend machen können. Diese Prozesse sind zu dokumentieren.

Sie hat zudem darauf hingewiesen, dass Prozesse für die Aufbewahrung und sichere Löschung der mit dem System bearbeiteten Informationen definiert werden müssen. Betroffene müssen auf Verlangen Zugang zu den sie betreffenden Datenbearbeitungen erhalten und die weiteren Rechte gemäss IDG geltend machen können. Diese Prozesse sind zu dokumentieren.

Da mit dem vorgesehenen System regelmässig besondere Personendaten bearbeitet werden, sind verschiedene technische und organische Massnahmen zum Schutz der Vertraulichkeit zu ergreifen. Dazu gehören die angemessene Einschränkung und der Schutz von Serverzugriffen (Authentifizierung und technische Netzwerksicherheitsmassnahmen), die Authentifizierung von Verbindungen zwischen GIFS und Umsystemen, der Schutz vor externen Zugriffen durch eine starke Authentifizierung (2-Faktor-Authentifizierung), die Zusammenführung der Protokolle (Log-Daten) auf einem zentralen, speziell gehärteten Server sowie deren kontinuierliche, automatisierte oder regelmässige und risikobasierte Auswertung.

Verhältnismässigkeit erklärt

Dauerüberwachung im Isolationszimmer von Pflegeheimen

Ein Pflegeheim installierte im Isolationszimmer eine dauerhafte Videoüberwachung. Die Aufnahmen wurden in Echtzeit sowohl auf einen grossen Bildschirm im Stationszimmer als auch auf die Mobiltelefone der Pflegedienstleitenden sowie der Heimleitung übertragen.

Beim betroffenen Isolationszimmer handelte es sich um einen kleinen Raum, der dem Schutz der dort wohnenden Person selbst sowie Dritter dient. Die Videoüberwachung umfasste den gesamten Raum, also auch den Toilettenbereich. Die Datenschutzbeauftragte schätzte die dauerhafte Videoüberwachung generell als einen schwerwiegenden Eingriff ein. Erschwerend kam hinzu, dass es sich bei dieser Art der Videoüberwachung um die Aufnahme einer heimbewohnenden Person in ihrem Alltag handelte. Solche Personen befinden sich in einer vulnerablen Situation und können ungewollt tiefe Einblicke in ihre Privatsphäre geben. Die Überwachung des Toilettenbereichs stellte einen Eingriff in die Intimsphäre der betroffenen Person dar. Diese Faktoren berücksichtigte die Datenschutzbeauftragte bei der Verhältnismässigkeitsprüfung.

Die Datenschutzbeauftragte schätzte die dauerhafte Videoüberwachung generell als einen schwerwiegenden Eingriff in die Privatsphäre der Heimbewohnenden ein.

Eine dauerhafte Videoüberwachung des Isolationszimmers erscheint als grundsätzlich geeignet für den Schutz aller Beteiligten. Die Erforderlichkeit einer solchen Massnahme ist jedoch zweifelhaft. Es ist durch das Heim zu klären, inwiefern eine solche Überwachung die Sicherheit der betroffenen Personen tatsächlich besser sicherstellen kann als beispielsweise der bereits im Pflegeheim etablierte Kontrollgang von Mitarbeitenden oder der Einsatz von Raumsensoren. Eine zeitliche Beschränkung der Videoüberwachung auf gefährliche Situationen wäre ein milderes Mittel. Die dauerhafte Überwachung eines Isolationszimmers ist deshalb in aller Regel nicht erforderlich. Weiter kam die Datenschutzbeauftragte zum Schluss, dass eine solche Überwachung für die betroffene Person grundsätzlich nicht zumutbar ist: Die Überwachung des Toilettenbereichs ist aufgrund des Eingriffs in die Intimsphäre an besondere Voraussetzungen geknüpft. Diese darf nur stattfinden, wenn eine ernste und unmittelbare Gefahr nicht anders abgewendet werden kann. Sie ist allenfalls ausschliesslich in einer absoluten Ausnahmesituation zulässig. Die Videoüberwachung im vorliegenden Fall war somit nicht verhältnismässig.

Darüber hinaus hat die Datenschutzbeauftragte auf weitere Grundsätze des Datenschutzrechts hingewiesen. So gelten die Prinzipien der Datenminimierung, der Vertraulichkeit und der Zweckbindung. Es dürfen deshalb nur diejenigen Personen Zugang zu einer solchen Videoüberwachung haben, für die der Zugriff auch unmittelbar notwendig ist. Dazu zählt grundsätzlich nur das ärztliche und pflegerische Personal vor Ort, das für die Betreuung und Behandlung der Bewohnenden zuständig ist. Ein Zugriff via Mobiltelefon der Heimleitung widerspricht diesen Grundsätzen, sofern diese nicht direkt für die Betreuung der betroffenen Person zuständig ist. Zudem wurden die Personendaten, die dem Berufsgeheimnis unterliegen, durch die Übertragung auf einen grossen Bildschirm im Stationszimmer sowie auf die Mobiltelefone der Heimleitung einem grossen Risiko ausgesetzt. Dabei war für die Datenschutzbeauftragte nicht ersichtlich, weshalb eine derartig grossflächige Übertra-

gung notwendig war. Das Prinzip der Datensparsamkeit erfordert, dass nicht notwendige Übertragungen verhindert werden.

Meldeformular für die Haltung von Rottweilern

Seit Anfang 2025 unterliegt die Haltung von Rottweilern im Kanton Zürich neuen Regeln. Wer einen solchen Hund halten will, muss ein detailliertes Gesuchsformular beim kantonalen Veterinäramt einreichen.

Halterinnen und Halter von Rottweilern meldeten sich bei der Datenschutzbeauftragten mit dem Bedenken, dass eine Beantwortung der Fragen im Formular zu tiefe Einblicke in ihr Privatleben gewähren würde. Gefragt wurde neben der Identität der Halterin oder des Halters auch nach dem Arbeitgeber, der Wohnsituation, einer Liste aller Personen mit regelmässigem Kontakt zum Hund und danach, welche Personen mit dem Tier spazieren gehen. Ein derartiger Katalog verletze nach Ansicht der betroffenen Personen den Grundsatz der Verhältnismässigkeit sowie die informationelle Selbstbestimmung. Weder für die Frage, ob sie als Halterinnen und Halter geeignet sind, noch für die Überprüfung, wie hoch das Gefährdungspotenzial ihres Hundes ist, sei der Fragekatalog geeignet und erforderlich.

Ob die Fragen in ihrer Art und ihrem Umfang geeignet und erforderlich sind, hat das Veterinäramt als vollziehendes öffentliches Organ selbst einzuschätzen. Es trägt die Verantwortung für die Einhaltung des Verhältnismässigkeitsgrundsatzes.

Die Datenschutzbeauftragte trat in Kontakt mit dem Veterinäramt, dem für den Vollzug des Hundegesetzes verantwortlichen öffentlichen Organ. Ob die Fragen in ihrer Art und ihrem Umfang geeignet und erforderlich sind, hat das Veterinäramt als vollziehendes öffentliches Organ selbst einzuschätzen. Es trägt die Verantwortung für die Einhaltung des Verhältnismässigkeitsgrundsatzes. Die Datenschutzbeauftragte beriet das Veterinäramt dahingehend, dass die Interessen der öffentlichen Sicherheit den datenschutzrechtlichen Interessen der betroffenen Hundehalterinnen und Hundehalter im Rahmen einer Interessenabwägung gegenüberzustellen sind. Dort, wo der Schutz der öffentlichen Sicherheit und der Vollzug der Hundegesetzgebung überwiege, dürfe das Veterinäramt in die Grundrechte der betroffenen Personen eingreifen. Die Verantwortung dieser Interessenabwägung liegt dabei beim Veterinäramt. Das Veterinäramt darf nur jene Personendaten mit dem Formular erheben, die zwingend für die Erfüllung der Hundegesetzgebung notwendig sind.

So erläuterte die Datenschutzbeauftragte, dass die Angabe des Arbeitgebers nicht als freiwillig deklariert werden darf. Entweder sei diese Angabe für die Beurteilung des Gesuchs der betroffenen Hundehalterinnen und Hundehalter notwendig und gehöre zwingend in das Formular, oder sie sei nicht notwendig. In diesem Fall dürfe sie keinen Eingang in das Formular finden. Eine solche Abwägung sei durch das Veterinäramt für jede einzelne Frage vorzunehmen. Das Veterinäramt legte der Datenschutzbeauftragten dar, inwiefern die Beantwortung sämtlicher Fragen im Katalog notwendig sei, um sowohl die Eignung der Halterin oder des Halters als auch das Risikopotenzial des Hundes zu eruieren. Nur die ganzheitliche Betrachtung der im Formular geforderten Angaben erlaube es dem Veterinäramt, die mit dem Hundegesetz und der dazugehörigen Hundeverordnung übertragenen Aufgaben vollständig und wirksam auszuüben und einen angemessenen Entscheid über die Bewilligung des Gesuches zu fällen.

Die Verwaltung von Personendaten durch Gemeinden

Im Jahr 2025 wandten sich vermehrt Gemeinden an die Datenschutzbeauftragte mit der Frage, ob und in welcher Form die Zugriffskonzepte von Geschäftsverwaltungssystemen so ausgestaltet werden können, dass eine abteilungsübergreifende Einsicht in die Geschäfte ermöglicht wird.

Öffentliche Organe des Kantons Zürich und die Gemeinden haben beim Umgang mit Informationen die Vorgaben des Gesetzes über die Information und den Datenschutz (IDG) zu achten. Im Kontext der Ausgestaltung von internen Zugriffsberechtigungen ist die Bestimmung zur Informationssicherheit sowie der Grundsatz der Verhältnismässigkeit hervorzuheben.

Die Informationen eines öffentlichen Organs sind durch angemessene technische und organisatorische Massnahmen zu schützen, insbesondere gegen unbefugte Zugriffe. Hierbei ist insbesondere darauf zu achten, dass die Informationen nicht Unberechtigten zur Kenntnis gelangen. Die Vertraulichkeit ist dabei auch innerhalb eines öffentlichen Organs zu gewährleisten. Der Zugriff auf Personendaten in den einzelnen Bereichen (Abteilungen, Ämter, Fachstellen etc.) der Gemeinde ist deswegen auf diejenigen Mitarbeitenden zu beschränken, die sie zur Erfüllung ihrer Aufgaben benötigen. Das Schutzziel der Vertraulichkeit wird insbesondere durch die Definition und Vergabe von restriktiven Berechtigungen erreicht.

Aus dem Grundsatz der Verhältnismässigkeit lässt sich ableiten, dass Mitarbeitende nur auf diejenigen Informationen Zugriff erhalten, welche für ihre eigene Aufgabenerfüllung notwendig sind. Der Zugriff auf Systeme und Anwendungen erfolgt somit nur nach vordefinierten Rollen und Berechtigungen. Die Berechtigungen werden nach dem Need-to-know-Prinzip vergeben: Die Gemeinden haben sicherzustellen, dass jede Mitarbeiterin und jeder Mitarbeiter nur jene Zugriffsrechte erhält, die für ihre oder seine Funktion und Tätigkeit erforderlich sind. Ein offenes Zugriffskonzept einzuführen, in dem die Mitarbeitenden abteilungsübergreifend Zugänge hätten, ist somit nicht mit den datenschutzrechtlichen Vorgaben vereinbar.

Der Zugriff auf Personendaten in den einzelnen Bereichen (Abteilungen, Ämter, Fachstellen etc.) der Gemeinde ist deswegen auf diejenigen Mitarbeitenden zu beschränken, die sie zur Erfüllung ihrer Aufgaben benötigen.

Da die Pflicht zur Vertraulichkeit innerhalb eines öffentlichen Organs und zwischen den einzelnen Bereichen gilt, muss sie erst recht zwischen verschiedenen öffentlichen Institutionen bestehen. Dies betrifft auch die Lösungen für das Personalwesen. Ist eine strikte Trennung der Personendaten zwischen verschiedenen Institutionen nicht möglich, sind nach dem Need-to-know-Prinzip einzelne Mitarbeitende zu bezeichnen, die für ihre Aufgabenerfüllung zwingend auf den Zugriff angewiesen sind. Die Zahl der berechtigten Personen ist auf das absolut notwendige Minimum zu begrenzen. Die Berechtigten sind in einer internen Weisung als solche zu bezeichnen. Diese Mitarbeitenden sind dahingehend zu schulen, dass sie immer nur die ihren Aufgabenbereich betreffenden Daten abrufen.

Die organisatorische Beschränkung von Einsichtsrechten durch die manuelle Vergabe von Zugriffsberechtigungen an einzelne Mitarbeitende stellt jedoch eine Notlö-

sung dar. Sobald technisch möglich, beispielsweise durch neue und beschränkte Berechtigungsprofile, ist eine strikte Trennung vorzunehmen und auf ein systematisches Rollenkonzept umzustellen.

Externe Gesundheitsdienstleistungen im Pflegeheim

Die multidisziplinäre Betreuung betagter und mobilitätseingeschränkter Personen birgt Herausforderungen. Im Pflegealltag werden häufiger ergänzende Behandlungen wie Physiotherapie vor Ort im Pflegeheim erbracht. Dabei kann es angezeigt sein, dass Physiotherapeutinnen und Physiotherapeuten über bestimmte gesundheitliche Voraussetzungen informiert werden. Gleichzeitig untersteht das Pflegepersonal dem Berufsgeheimnis.

Im Jahr 2025 hat sich ein Pflegeheim an die Datenschutzbeauftragte gewandt und sich zu den datenschutzrechtlichen Rahmenbedingungen für die regelmässige Erbringung von Physiotherapie vor Ort informiert. Konkret standen der Zugang der Physiotherapiepraxis zur Pflegedokumentationssoftware des Heims sowie die dort gemeinsam verwaltete Dokumentation der Pflege und der Physiotherapiebehandlung im Fokus. Dieses Vorgehen würde eine Bekanntgabe besonderer Personendaten und eine Durchbrechung des Berufsgeheimnisses bedeuten. Für diese Konstellation wäre eine ausreichende gesetzliche Grundlage notwendig.

Die Datenschutzbeauftragte hat dem Pflegeheim die Option aufgezeigt, den Physiotherapeutinnen und Physiotherapeuten eine so umrissene und damit klar beschränkte Auskunft zu einzelnen Heimbewohnenden zu geben.

Die Datenschutzbeauftragte hat das Pflegeheim darüber informiert, dass für einen umfassenden Zugang und die gemeinsame Führung der Pflege- und Therapiedokumentation eine entsprechende Grundlage fehlt. Zum Wohl der behandelten Person besteht jedoch im Anwendungsbereich des Patientinnen- und Patientengesetzes die gesetzliche Vermutung, dass vor- und nachbehandelnde Ärztinnen und Ärzte sowie in geeigneter Weise auch andere weiterbehandelnde Personen über den Gesundheitszustand rechtzeitig zu informieren sind, sofern sich die betroffene Person nicht dagegen ausspricht. Die Datenschutzbeauftragte hat dem Pflegeheim daher die Option aufgezeigt, den Physiotherapeutinnen und Physiotherapeuten eine so umrissene und damit klar beschränkte Auskunft zu einzelnen Heimbewohnenden zu geben. Zu beachten ist dabei das Prinzip der Verhältnismässigkeit: Das Heim ist verpflichtet, nur diejenigen Daten weiterzugeben, die für die Physiotherapie erforderlich sind.

Datenschutz in Einheitsgemeinden: Wer trägt die Verantwortung?

In Einheitsgemeinden verschwimmen die organisatorischen Grenzen zwischen Schule und Gemeindeverwaltung. Wer bei der Bearbeitung von Personendaten tatsächlich verantwortlich ist, hängt jedoch nicht von der Struktur ab, sondern davon, wer entscheidet.

Neue organisatorische Realität

Eine grosse Mehrheit der Zürcher Gemeinden nimmt heute auch schulische Aufgaben wahr. Einheitsgemeinden sind zur Regel geworden, separate Schulgemeinden bilden die Ausnahme. Während in Schulgemeinden die Schulpflege als eigenständige Behörde für schulische Belange zuständig ist, sind Schule und Gemeindeverwaltung in Einheitsgemeinden organisatorisch enger miteinander verbunden. Diese Integration wirft auch Fragen zum Datenschutz auf – insbesondere hinsichtlich der datenschutzrechtlichen Verantwortung.

Einheitsgemeinden wurden unter anderem geschaffen, um Ressourcen effizienter zu nutzen und Personalengpässe flexibler auszugleichen. Entsprechend ist die Schulverwaltung heute oft Teil der Gemeindeverwaltung. Administrative Aufgaben werden gemeinsam wahrgenommen, Akteneinsichtsgesuche werden häufig bei der Gemeindeverwaltung bearbeitet. Diese Nähe kann den Eindruck erwecken, die Verantwortung liege bei der Gemeindeverwaltung. Tatsächlich ist die Situation differenzierter.

Schulische Aufgaben – schulische Verantwortung

Die Schule bearbeitet zahlreiche Personendaten, etwa zu Schülerinnen und Schülern oder Lehrpersonen. Soweit diese Bearbeitungen auf schulischen Entscheiden beruhen, liegt die Verantwortung bei der Schule.

Dies gilt insbesondere für gesetzlich zugewiesene Kompetenzen der Schulpflege, etwa beim Kerngeschäft der Schule, bei der Unterrichtsgestaltung sowie bei der Anstellung oder Entlassung von Mitarbeitenden. Auch wenn die Gemeindeverwaltung administrative Unterstützung bietet, bleibt die Verantwortung bei der Schule.

Auch wenn die Gemeindeverwaltung administrative Unterstützung bietet, bleibt die Verantwortung bei der Schule.

Gemeinsame Infrastruktur

In vielen Einheitsgemeinden werden IT-Systeme zentral durch die Gemeindeverwaltung betrieben. Die Schule nutzt diese Infrastruktur, ohne sie selbst wählen zu können. Die Schule kann nur für das verantwortlich sein, worüber sie entscheidet. Gibt

die Gemeindeverwaltung eine IT-Lösung vor, ohne dass die Schule Einfluss hat, trägt die Gemeindeverwaltung die Verantwortung für diese Entscheidung.

Die Schule bleibt jedoch verantwortlich für die Art und Weise der Nutzung der Systeme und die darin bearbeiteten Daten.

Klare Zuständigkeiten

Wesentlich ist die Entscheidungskompetenz: Die Schule ist für ihre Entscheide verantwortlich, die Gemeindeverwaltung für ihre. Klare Regelungen sind zentral für einen datenschutzkonformen Umgang mit Personendaten. Diese Zuständigkeiten sind eindeutig zu regeln, insbesondere bei IT und Administration. Dadurch ist die Verantwortung klar festgehalten und muss nicht durch Auslegung eruiert werden.

Zugang zu eigenen Personendaten bei öffentlichen Organen mit Querschnittsfunktion

Öffentliche Organe bearbeiten je nach gesetzlichem Auftrag Personendaten, die sie nicht selbst erhoben haben. Welches Organ ist in dieser Konstellation für die Behandlung von Auskunftsgesuchen zuständig?

Die Ombudsstelle des Kantons Zürich ist Teil der Aufsichtsbehörden, die das Verwaltungshandeln kontrollieren. In dieser Funktion nimmt sie fallweise eine Vermittlungsrolle zwischen der Verwaltung und Privatpersonen ein. Bei der Behandlung konkreter Fälle erhält sie Zugang zu den relevanten Informationen und damit auch zu Personendaten, die das öffentliche Organ in diesem Zusammenhang bearbeitet hat. Vor diesem Hintergrund hatte die Datenschutzbeauftragte im Jahr 2025 folgende Frage zu klären: Hat eine mit einer Querschnittsaufgabe betraute Behörde wie die Ombudsstelle datenschutzrechtliche Auskunftsgesuche zu behandeln, auch wenn sie die betreffenden Personendaten nicht selbst erhoben und nur im Rahmen ihrer Vermittlungsrolle erhalten hat?

Dabei ist es unerheblich, ob das angefragte öffentliche Organ diese Daten selbst verfasst oder lediglich zur Aufgabenerfüllung erhalten hat: Solange eine Behörde Personendaten bearbeitet, besteht der grundrechtlich geschützte Anspruch betroffener Personen, dies auf Gesuch hin in Erfahrung bringen zu können.

Öffentliche Organe im Kanton Zürich tragen in ihrem gesetzlich zugewiesenen Zuständigkeitsbereich die Verantwortung für eine Bearbeitung von Personendaten gemäss den Grundsätzen des Gesetzes über die Information und den Datenschutz (IDG). Aufgrund des weit gefassten Begriffs der Bearbeitung – jeder Umgang mit Personendaten – bezieht sich die Verantwortung auch auf solche Personendaten, die ein öffentliches Organ zwar nicht originär selbst erhoben, aber im Rahmen seiner Aufgabenerfüllung von einer anderen Stelle erhalten hat. Die datenschutzrechtliche Verantwortung bedeutet unter anderem, dass das öffentliche Organ dem individuellen Anspruch betroffener Personen auf Zugang zu den eigenen Personendaten entsprechend den Vorgaben des IDG nachkommen muss. Das Auskunftsrecht verfolgt gerade den Zweck, dass die betroffene Person erfährt, welche Behörde Daten zu ihrer Person bearbeitet. Dabei ist es unerheblich, ob das angefragte öffentliche Organ diese Daten selbst verfasst oder lediglich zur Aufgabenerfüllung erhalten hat: Solange eine Behörde Personendaten bearbeitet, besteht der grundrechtlich geschützte Anspruch betroffener Personen, dies auf Gesuch hin in Erfahrung bringen zu können.

Damit ist auch eine Institution wie die Ombudsstelle verpflichtet, Auskunftsgesuche zu den in ihrem Aufgabenbereich bearbeiteten Personendaten zu behandeln. Es bietet sich aber in der Regel an, die ursprüngliche Behörde für die konkrete Prüfung eines Auskunftsgesuch zu konsultieren. Auskunftgsgesuche können abgelehnt oder aufgeschoben werden, wenn der Bekanntgabe eine rechtliche Bestimmung oder überwiegende öffentliche oder private Interessen entgegenstehen.

Webscanning

Erste Kontrolle einer KI-Applikation

Künstliche Intelligenz (KI) kommt zunehmend auch bei öffentlichen Organen des Kantons Zürich zum Einsatz. So setzen diese zunehmend Chatbots ein, um Fragen der Bevölkerung automatisch zu beantworten. Solche Systeme sollen den Aufwand der Verwaltung reduzieren und einfache Anfragen rasch beantworten, zum Beispiel zur Abfallentsorgung oder zu Fristen bei Steueranangelegenheiten.

Zahlreiche öffentliche Organe haben in den letzten Jahren solche Systeme eingeführt, ohne dass zuvor eine Vorabkontrolle bei der Datenschutzbeauftragten stattgefunden hat. Den Einsatz solcher Anwendungen beurteilen öffentliche Organe oft als unkritisch, weil sie nur mit öffentlich zugänglichen Informationen arbeiten und keine Entscheidungen treffen. Jedoch zeigen weltweite Vorfälle, wie scheinbar einfache KI-Applikationen datenschutzrechtliche Risiken mit sich bringen. Vor diesem Hintergrund führte die Datenschutzbeauftragte eine Kontrolle eines solchen Systems durch.

Der Einsatz von Chatbots kann datenschutzrechtliche Risiken mit sich bringen. Die Systeme arbeiten in der Regel mit Freitextfeldern. Nutzerinnen und Nutzer formulieren ihre Anliegen dort häufig so, wie sie diese auch einer Mitarbeiterin oder einem Mitarbeiter einer Behörde schildern würden. Dabei können auch sensitive Personendaten eingegeben werden, zum Beispiel AHV-Nummern oder persönliche Angaben zu individuellen Anliegen, selbst wenn dies für die Nutzung des Chatbots nicht vorgesehen ist. Zudem kann der Eindruck entstehen, dass die Kommunikation besonders vertrauenswürdig ist, weil ein öffentliches Organ hinter dem Angebot steht.

Viele Chatbots basieren auf kommerziellen KI-Modellen externer Anbieter. Werden dabei Daten an Dritte übermittelt, handelt es sich datenschutzrechtlich um eine Auftragsdatenbearbeitung.

Der von der Datenschutzbeauftragten geprüfte Chatbot beantwortet einfache Anfragen von Besucherinnen und Besuchern der Website. Er hilft dabei, Informationen auf der Website schneller zu finden, zum Beispiel zu Dienstleistungen oder Zuständigkeiten.

Der Chatbot arbeitet ausschliesslich mit öffentlichen Informationen. Er greift auf Inhalte zu, die bereits auf der Website des öffentlichen Organs publiziert sind. Ein Zugriff auf interne Systeme oder nicht öffentliche Daten ist nicht vorgesehen. Dennoch besteht ein Risiko: Werden vertrauliche Informationen versehentlich auf der Website veröffentlicht, kann der Chatbot diese Inhalte ebenfalls aufgreifen und in Antworten wiedergeben. Dadurch könnten sensitive Informationen einfacher gefunden und abgefragt werden als auf der Website selbst.

Die Kontrolle umfasste eine Prüfung der datenschutzrechtlichen Rahmenbedingungen des Chatbots. Geprüft wurden insbesondere die vertraglichen Grundlagen sowie die organisatorischen und technischen Rahmenbedingungen des Einsatzes.

Die Kontrolle zeigte, dass Chatbots besondere Herausforderungen für den Datenschutz und auch für die öffentlichen Organe mit sich bringen.

Zu diesem Zweck prüfte die Datenschutzbeauftragte die vorhandenen Unterlagen zum System. Es wurde insbesondere geprüft, ob die Applikation getestet und dokumentiert wurde, wer Zugriff auf das System hat und wie dieser Zugriff ausgestaltet ist sowie welche vertraglichen Regelungen bestehen.

Bei Gesprächen mit den verantwortlichen Mitarbeitenden zeigte sich, dass die Applikationen nicht über den vorgesehenen Beschaffungsprozess eingeführt wurden. Da der Chatbot nur mit öffentlich zugänglichen Informationen arbeitet, wurde das System als unkritisch eingestuft. Dadurch wurden Risiken teilweise unterschätzt oder nicht systematisch beurteilt.

Die Kontrolle zeigte aber keine Hinweise auf Konfigurationsfehler. Der Chatbot greift nur auf die vorgesehenen Daten zu. Für die Veröffentlichung von Informationen auf der Website besteht ein definierter Prozess, der sicherstellt, dass nur geprüfte Inhalte in den Datenbestand des Chatbots gelangen.

Die Kontrolle offenbarte mehrere Punkte, bei denen Verbesserungen notwendig sind.

Für den Einsatz des Systems fehlen klar geregelte vertragliche Grundlagen mit den eingesetzten Diensten. Dadurch bleibt teilweise unklar, unter welchen Rahmenbedingungen Daten bearbeitet werden.

Zudem ist die Anbindung an externe Dienste nur begrenzt nachvollziehbar. Anforderungen an Transparenz und Nachvollziehbarkeit der Datenbearbeitung sind nicht klar definiert.

Schliesslich bestehen auch technische Risiken, die für KI-Systeme typisch sind. Dazu gehören insbesondere fehlerhafte Antworten (Halluzinationen) sowie mögliche Manipulationen der Eingaben, zum Beispiel durch sogenannte Prompt-Injection-Angriffe. Dabei versuchen Nutzerinnen oder Nutzer, das System mit gezielten Eingaben zu beeinflussen oder zu missbrauchen, etwa um unerwünschte Inhalte auszugeben, zweckfremde Aufgaben zu erledigen oder Schutzmechanismen zu umgehen.

Aufgrund dieser Feststellungen hielt die Datenschutzbeauftragte verschiedene Massnahmen fest.

Zunächst sind die vertraglichen Grundlagen mit den eingesetzten Diensten kritisch zu prüfen. Insbesondere ist zu klären, unter welchen Bedingungen Daten bearbeitet werden und welche Pflichten für die beteiligten Anbieter gelten.

Weiter empfahl sie, organisatorische und technische Massnahmen zur Überwachung des Systems zu ergreifen. Dazu gehört insbesondere eine Kontrolle der Nutzung, damit ungewöhnliche oder missbräuchliche Verwendungen frühzeitig erkannt werden können. Zudem sollten geeignete Massnahmen zum Schutz gegen Manipulationen der Eingaben umgesetzt werden.

Die Kontrolle zeigte, dass Chatbots besondere Herausforderungen für den Datenschutz und auch für die öffentlichen Organe mit sich bringen. Freitextfelder laden Nutzerinnen und Nutzer dazu ein, auch sensitive Personendaten einzugeben. Zudem ist für viele Personen nicht immer klar, ob sie mit einem automatisierten System oder mit einer Auskunftsstelle eines öffentlichen Organs kommunizieren.

Sie zeigte auch, dass die vertraglichen Grundlagen mit den eingesetzten Diensten sorgfältig geprüft werden müssen. Viele Anbieter behalten sich vor, eingegebene Daten für eigene Zwecke zu verwenden, zum Beispiel zur Verbesserung ihrer Produkte.

Beim Einsatz von Chatbots bleibt das öffentliche Organ für die Bearbeitung der Daten verantwortlich, auch wenn die technische Lösung von einem externen Dienstleister bereitgestellt wird.

Weiter ist zu berücksichtigen, dass KI-Systeme fehlerhafte Antworten geben können. Nutzerinnen und Nutzer sollten deshalb erkennen können, dass sie mit einer KI-Applikation kommunizieren. Zudem sollte klar sein, wo fehlerhafte Antworten gemeldet werden können.

Schliesslich können auch aus öffentlich publizierten Informationen Rückschlüsse auf einzelne Personen gezogen werden. Bei der Verwendung solcher Daten durch Chatbots ist deshalb besondere Sorgfalt erforderlich.

Datenschutz-Reviews in Primar- und Sekundarschulen

Aufgrund der laufenden Digitalisierung steigen die Anforderungen an die organisatorischen und technischen Massnahmen, um den Schutz der Privatsphäre von Schülerinnen und Schülern sowie Lehrpersonen zu gewährleisten. Dabei wird von den Schulen eine Vielzahl sensitiver Daten in Form von Lernfortschritten oder heilpädagogischen Sondermassnahmen bearbeitet.

Die Datenschutzbeauftragte hat im Jahr 2025 den Schwerpunkt bei den Kontrollen auf Schulen gelegt. Aufgrund der einfacheren Verwaltung werden die Daten dabei vermehrt in Software as a Service (SaaS) und in Cloud-Lösungen bearbeitet. Um den erfolgreichen Schutz der Privatsphäre zu gewährleisten, sind entsprechende organisatorische, technische und rechtliche Massnahmen unabdingbar.

Das primäre Ziel der Datenschutz-Reviews war eine Ermittlung des aktuellen Umsetzungsstands technischer und organisatorischer Massnahmen an den Schulen, orientiert am Stand der Technik gemäss dem Gesetz über die Information und den Datenschutz (IDG). Dabei wurde festgestellt, dass die Schulen dem Datenschutz eine hohe Priorität beimessen – vor allem durch gute organisatorische Massnahmen. Dies zeigt sich beispielsweise durch vorhandene Weisungen, welche den Umgang mit Fotos von Schulkindern oder das Speichern von sensitiven Daten regeln. Zudem sind heilpädagogische Sondermassnahmen in fast allen kontrollierten Schulen nicht digitalisiert, sondern als Papierakten verschlossen abgelegt.

Das primäre Ziel der Datenschutz-Reviews war eine Ermittlung des aktuellen Umsetzungsstands technischer und organisatorischer Massnahmen an den Schulen, orientiert am Stand der Technik gemäss IDG.

Dagegen fehlten in vielen Fällen wichtige technische Massnahmen. Dies zeigte sich vor allem in der Abwesenheit von Grundlagen und Konzepten im Bereich der Informationssicherheit. Verbesserungspotenzial besteht insbesondere bei der IKT-Risikoanalyse, der Schutzbedarfsanalyse, der Informationssicherheitsleitlinie, dem Informationssicherheitskonzept, der Informationsklassifizierung, dem Rollen- und Berechtigungskonzept, den IKT-Weisungen für die Benutzenden, dem Back-up-Konzept, den Vorgaben zur sicheren Konfiguration der IKT-Systeme, dem Prozess für Security Incident Management (IM) sowie dem Schwachstellenmanagement.

Deshalb wurden bislang in den wenigsten Schulen Schulungen oder Sensibilisierungsmassnahmen im Bereich der Informationssicherheit durchgeführt.

Um die Schulen bei der Implementierung sowie bei der kontinuierlichen Verbesserung im Informationssicherheitsmanagement zu unterstützen, stellt die Datenschutzbeauftragte auf ihrer Website zahlreiche Merkblätter und Vorlagen zur Verfügung. Zudem tauschen sich die Datenschutzbeauftragte und das Volksschulamt regelmässig aus, um den Schulen eine angepasste Unterstützung zu bieten.

Kontrolle beim Visa-Informationssystem (VIS)

Die Datenschutzbeauftragte kontrollierte den Einsatz des Visa-Informationssystems (VIS) in einer Zürcher Gemeinde mit Fokus auf die Rechtmässigkeit der Zugriffe sowie organisatorische Anforderungen. Positiv ist festzuhalten, dass keine unrechtmässigen Zugriffe auf das VIS erkannt wurden. Mängel wurden im Bereich der Sensibilisierungsmassnahmen festgestellt. Diese behob die verantwortliche Stelle zeitnah.

Kontrolle des Generalsekretariats einer Direktion

Bei der Kontrolle des Generalsekretariats einer Direktion fand die Datenschutzbeauftragte eine umfassende Informationssicherheitsorganisation und eine sehr hohe Sensibilisierung der Mitarbeiterinnen und Mitarbeiter, aber auch fehlende Prozesse zu Datenschutz und Informationssicherheit vor.

Im Jahr 2025 hat die Datenschutzbeauftragte wie bereits im Vorjahr eine Kontrolle des Generalsekretariats einer Direktion mit Fokus auf die Prozesse und Vorgaben zum Datenschutz und zur Informationssicherheit durchgeführt. Dabei fand sie eine umfassende Informationssicherheitsorganisation und eine sehr hohe Sensibilisierung der Mitarbeitenden im Hinblick auf Informationssicherheitsrisiken vor. Ebenso positiv zu bewerten war die gute Übersicht über die Schutzobjekte der direktionseigenen IKT-Systeme. Verbesserungspotenzial hat die Datenschutzbeauftragte bezüglich verschiedener fehlender Prozesse zur Umsetzung der Datenschutz- und Informationssicherheitsanforderungen festgestellt.

Prüfung der Formerfordernisse für die Auskunftserteilung zu eigenen Personendaten

Nach Anfrage einer Privatperson hat die Datenschutzbeauftragte bei einer Zürcher Behörde überprüft, wie diese die Auskunftserteilung zu eigenen Personendaten handhabt. Ein öffentliches Organ muss jeder Person auf schriftliches Gesuch hin Zugang zu den eigenen Personendaten gewähren.

Um sicherzustellen, dass das öffentliche Organ ausschliesslich der betreffenden Person Zugang zu deren Personendaten verschafft, hat sich die gesuchstellende Person zu identifizieren. In der Kontrolle stellte die Datenschutzbeauftragte fest, dass die Behörde geeignete Massnahmen zur Prüfung der Identität vorsieht. Die Behörde prüft die Identität der gesuchstellenden Person durch das Verlangen eines Identitätsnachweises und durch die Abfrage spezifischer Dossierkenntnisse.

Als Grundsatz sieht das Gesetz eine schriftliche Auskunftserteilung in Form eines Ausdrucks oder einer Fotokopie vor. Das öffentliche Organ kann die Auskunft auch mündlich erteilen, wenn dies für den Umfang der Auskunftserteilung geeignet ist. Die Auskunftserteilung auf elektronischem Weg darf nur mit Zustimmung der gesuchstellenden Person erfolgen.

Die Datenschutzbeauftragte stellte jedoch fest, dass die Form der Auskunftserteilung nicht den gesetzlichen Vorgaben entsprach. Als Grundsatz sieht das Gesetz eine schriftliche Auskunftserteilung in Form eines Ausdrucks oder einer Fotokopie vor. Das öffentliche Organ kann die Auskunft auch mündlich erteilen, wenn dies für den Umfang der Auskunftserteilung geeignet ist. Die Auskunftserteilung auf elektronischem Weg darf nur mit Zustimmung der gesuchstellenden Person erfolgen. Die Behörde führte jedoch eine ausschliesslich elektronische Auskunftserteilung durch. Eine solche ist gegen den Willen der gesuchstellenden Person unrechtmässig.

Die Behörde reagierte auf die Feststellungen der Datenschutzbeauftragten und wird die Formerfordernisse der Auskunftserteilung nach den gesetzlichen Vorgaben anpassen.

Angriffe auf die Datensicherheit

Im Rahmen der Meldepflicht bei Datenschutzverletzungen wurden der Datenschutzbeauftragten im Jahr 2025 diverse Meldungen eingereicht. Mehrere Meldungen bezogen sich auf erfolgreich durchgeführte Angriffe durch Dritte auf die betroffenen öffentlichen Organe oder deren Lieferanten. Beobachtet wurden insbesondere Angriffe mittels Ransomware sowie die Entwendung von Zugangsdaten mittels Social-Engineering-Angriffen.

Bei den meisten Ransomware-Angriffen geht es darum, mittels verschlüsselter oder gestohlener Daten Geld zu erpressen. Nach dem Angriff verlangen die Angreifenden Geld, um die Daten wieder zu entschlüsseln oder um deren Veröffentlichung (zum Beispiel im Darknet) zu verhindern. Zunehmend werden ausserdem die entwendeten Daten verwendet, um die betroffenen Personen zusätzlich direkt zu erpressen.

Bei Social-Engineering-Angriffen versuchen Angreifende, Mitarbeitende öffentlicher Organe zur Ausführung bestimmter Handlungen zu bringen. Die Ziele eines solchen Angriffs können sehr vielfältig sein, von der Ausführung von Malware über die Kundgabe von Zugangsdaten bis zur Bekanntgabe von internen Informationen und Daten. Oft finden die Angriffe via E-Mail oder Telefon statt.

Erhält die Datenschutzbeauftragte eine Meldung über einen Angriff auf die Datensicherheit, berät sie das öffentliche Organ bei der Bewältigung und fordert, wenn nötig, die Umsetzung zusätzlicher Massnahmen, um die Informationssicherheit der betroffenen Organisation zu erhöhen und das Risiko zukünftiger Datenschutzverletzungen zu reduzieren.

Das Risiko eines erfolgreichen Angriffs kann durch entsprechende Massnahmen reduziert werden. Die konkrete Ausgestaltung hängt stark von der jeweiligen Situation beim öffentlichen Organ ab. Im Folgenden werden einige wichtige Massnahmen vorgestellt:

- Sicherheitsrelevante Prozesse sollten klar definiert und unter Berücksichtigung der Anforderungen der Informationssicherheit und des Datenschutzes ausgestaltet sein. Die Mitarbeitenden sollten bezüglich dieser Prozesse geschult und auf die Erkennung üblicher Angriffe sensibilisiert werden.
- Die Prozesse und Vorgaben der Benutzerverwaltung und des Berechtigungsmanagements sind klar zu definieren. Dabei sind die Berechtigungen aller Benutzenden auf ein Minimum zu reduzieren und regelmässig zu überprüfen.
- Eine starke Authentisierung ist konsequent umzusetzen.
- Die Informations- und Kommunikationstechnik (IKT-Systeme) ist durch technische Massnahmen zu schützen. Dazu gehört insbesondere das zeitnahe Installieren von Updates, die umfassende Protokollierung, der Schutz der Log-Daten, das Monitoring von sicherheitsrelevanten Aktivitäten (SIEM), die sichere Konfiguration der Systeme (Härtung) sowie Datensicherungen (Back-ups).
- Das Durchführen von Security Reviews zur Identifikation von Schwachstellen und der damit verbundenen Risiken in den IKT-Systemen.
- Daten auf (mobilen) Speichermedien und bei der Übertragung sind zu verschlüsseln. Für die Verschlüsselung müssen sichere kryptographische Verfahren eingesetzt werden, beispielsweise nach der Technischen Richtlinie des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI TR-02102).

Sicherheitsrelevante Prozesse sollten klar definiert und unter Berücksichtigung der Anforderungen der Informationssicherheit und des Datenschutzes ausgestaltet sein. Die Mitarbeitenden sollten bezüglich dieser Prozesse geschult und auf die Erkennung üblicher Angriffe sensibilisiert werden.

Da keine absolute Sicherheit möglich ist, sind neben Massnahmen zum direkten Schutz vor Angriffen auch Massnahmen zur Reduktion der Auswirkungen und zur Detektion von Angriffen sowie zur Wiederherstellung des Geschäftsbetriebes erforderlich. Generell ist es empfehlenswert, sich an anerkannte Standards und Frameworks zu richten. Diese helfen bei der Definition und Ausgestaltung von Massnahmen und bieten eine gewisse Sicherheit, dass keine wichtigen Bereiche vergessen wurden. Dazu zählen beispielsweise:

- Standards der ISO/IEC 27000-er Reihe, insbesondere 27001 und 27002,
- IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI),
- Cybersecurity Framework (CSF) des National Institute for Standards and Technology (NIST),
- IKT-Minimalstandard des Schweizerischen Bundesamts für Cybersicherheit (BACS).

Empfehlungen der PUK Datensicherheit

Die Parlamentarische Untersuchungskommission Datensicherheit des Kantonsrats (PUK Datensicherheit) hat am 12. Dezember 2025 ihren Bericht mit zahlreichen Empfehlungen veröffentlicht. Diese sind auch relevant für die Aufgaben und Tätigkeiten der Datenschutzbeauftragten.

Aufgrund eines Datenschutzvorfalls bei der Direktion der Justiz und des Innern (JI) setzte der Kantonsrat die PUK Datensicherheit ein. In ihrem Bericht kommt sie zum Schluss, dass die Informationssicherheit in der kantonalen Verwaltung durch die gesetzlichen Grundlagen aus den 1990er Jahren bereits früh angemessen geregelt war, ihr aber über Jahre zu wenig Beachtung geschenkt wurde. Diese Feststellung deckt sich mit den Erkenntnissen der Datenschutzbeauftragten, wie dies sowohl in den Tätigkeitsberichten des durch die PUK Datensicherheit betrachteten Zeitraumes wie auch im Tätigkeitsbericht des Jahres 2022 zum Ausdruck kommt. Mit Nachdruck wurde in diesen Berichten immer wieder auf die Umsetzung der notwendigen Massnahmen hingewiesen.

Die PUK Datensicherheit stellt in ihrem Bericht auch in Bezug auf die Gegenwart weiterhin grosse Mängel bei den Grundlagen und in der Umsetzung der Datensicherheit in der kantonalen Verwaltung fest. Sie formuliert in ihrem Bericht deshalb 50 Empfehlungen an Regierungsrat und Kantonsrat, wie die Datensicherheit in Zukunft effizient umgesetzt werden kann.

Zu den Schwerpunkten der Tätigkeiten der Datenschutzbeauftragten gehören die Kontrollen, bei denen immer wieder Mängel im Bereich der Datensicherheit aufgedeckt werden. Kontrollen tragen damit zu einer wesentlichen Verbesserung der Datensicherheit bei. Diesen Beitrag der Kontrollen zur Datensicherheit sieht auch die PUK Datensicherheit und empfiehlt, diese wesentlich zu intensivieren. In der Empfehlung 49a sieht die PUK Datensicherheit die Stärkung der Kontrollaktivitäten der Datenschutzbehörde als Massnahme vor, zusammen mit einer erweiterten Berichterstattung an die kantonsrätlichen Aufsichtskommissionen. Aus Sicht der Datenschutzbeauftragten lässt sich eine umfassendere Kontrolltätigkeit ohne gesetz-liche Anpassungen rasch realisieren, wenn die notwendigen personellen Ressourcen der Behörde zur Verfügung gestellt werden. Eine ausführlichere Berichterstattung ist mit einer Anpassung auf Verordnungsebene möglich. Dagegen erscheinen die anderen Vorschläge, das Kerngeschäft der Finanzkontrolle zu erweitern (Empfehlung 49b) oder eine neue Behörde zu schaffen (Empfehlung 49c) nicht nur aufwändig, sondern in Bezug auf die Aufgaben der Finanzkontrolle wesensfremd und in Bezug auf die Schaffung einer neuen Behörde verwaltungsökonomisch fraglich.

Die transparente Berichterstattung gegenüber den Aufsichtskommissionen (Empfehlungen 44 ff.) ist auch ein Anliegen der Datenschutzbeauftragten. Die klare Festlegung von Prozessen, die Periodizität sowie Inhalt und Adressaten der Berichte liessen sich in einer Anpassung auf Verordnungsebene gleichzeitig realisieren.

Die PUK Datensicherheit empfiehlt im Weiteren, die Regelungen zur Informationssicherheit rechtlich stärker zu verankern (Empfehlung 9 ff.). Dabei geht es nicht nur um die Organisationstrukturen für die Informationssicherheit, sondern auch um die Festlegung der Grundsätze der Informationssicherheit auf Verordnungsebene (Empfehlung 13). Die Datenschutzbeauftragte unterstützt diese Zielrichtung, da nur so erreicht werden kann, dass ein einheitliches Sicherheitsniveau über die gesamte

Verwaltung gewährleistet ist. Zudem lassen sich Verantwortlichkeiten verbindlich festlegen.

Auch in Bezug auf die Konkretisierung der Massnahmen zur Datensicherheit (§ 7 IDG) sieht die PUK Datensicherheit Handlungsbedarf (Empfehlung 29). Diesem Anliegen kann mit der Anpassung der IDV im Rahmen des totalrevidierten IDG entsprochen werden. Ebenso lassen sich dabei die einschlägigen Allgemeinen Geschäftsbedingungen (AGB) des Kantons aktualisieren.

Spezifisch äussert sich die PUK Datensicherheit zu den Sicherheitsrisiken von Cloud-Lösungen (Empfehlungen 37 ff.). Mit Merkblättern und Leitfäden berät die Datenschutzbeauftragte die Verwaltung in diesem Bereich seit Jahren. Die PUK Datensicherheit unterstreicht, dass die Risiken von Cloud-Lösungen wie M365 sehr ernst zu nehmen sind. Sie empfiehlt sowohl eine Prüfung der Ablösung von M365 als auch eine verstärkte Unterstützung der Mitarbeitenden mit technischen Mitteln beim richtigen Umgang mit besonderen Personendaten. Damit wird den Anliegen des Datenschutzes die notwendige Nachachtung verschafft.

Dies kommt auch in der Empfehlung 41 zum Ausdruck: Die PUK Datensicherheit empfiehlt, dass auch gegenüber den selbständigen öffentlich-rechtlichen Anstalten im Rahmen der Eigentümerstrategie verbindliche Vorgaben zur Informationssicherheit gemacht und überprüft werden, was als Konkretisierung der allgemeinen Massnahmen des IDG zu begrüssen ist.

Die PUK Datensicherheit hat mit ihrer Analyse und ihren Empfehlungen einen wichtigen Beitrag zur Informationssicherheit geleistet. Die Datenschutzbeauftragte wird bei der Diskussion und Umsetzung der Erkenntnisse aus diesem Bericht die verantwortlichen Organe beratend und unterstützend begleiten.