dsb
datenschutzbeauftragte
des kantons zürich

Tätigkeitsbericht 2023

Vorwort

Die Datenschutzbeauftragte Dr. Dominika Blonski an der IT-Beschaffungskonferenz. Foto: Stefan Lehmann

Die Beauftragte 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 Tätigkeitsbericht deckt den Zeitraum vom 1. Januar 2023 bis und mit 31. Dezember 2023 ab.

Der 29. Tätigkeitsbericht erscheint ausschliesslich digital und wird unter www.datenschutz.ch *(https://www.datenschutz.ch/)* publiziert.

Digitalisierung besteht nicht nur aus vielen einzelnen IKT-Projekten. Mit der Digitalisierung geht eine eigentliche Verwaltungsreform, eine digitale Transformation einher. Vermehrt braucht es den Fokus auf das grosse Ganze.

Mängel und Abkürzungen beim Datenschutz und in der Informationssicherheit führen zum Verlust des Vertrauens der Bevölkerung.

Im Streben nach der raschen Veränderung schleichen sich vermehrt und wiederholt privatrechtliche Argumentationen in die Vorgehensweisen der öffentlichen Organe ein. Doch die Datenbearbeitungen im öffentlichen Sektor müssen den verfassungsmässig verbrieften Grundrechten entsprechen. Völlig unabhängig von der eingesetzten Technologie gehören Einwilligungen und rechtliche Risikoeinschätzungen hier nicht hin.

In ihren Kontrollen, aber auch durch die Meldungen von Datenschutzvorfällen stellt die Datenschutzbeauftragte grundlegende Mängel fest. Gerade angesichts der international zunehmenden Cyberrisiken ist die Umsetzung der datenschutzrechtlichen Vorgaben und der Massnahmen zur Informationssicherheit von höchster Bedeutung. Mängel und Abkürzungen in diesem Bereich führen zum Verlust des Vertrauens der Bevölkerung – und dieses Vertrauen ist essenziell, damit die öffentlichen Organe ihre Aufgaben erfüllen können.

Dr. Dominika Blonski
Datenschutzbeauftragte des Kantons Zürich

Privatrechtliche Argumentationen gehören nicht in den öffentlichen Sektor

Jede Bearbeitung von Personendaten ist ein Eingriff in die Persönlichkeitsrechte der Betroffenen, besonders das Grundrecht auf informationelle Selbstbestimmung. Öffentliche Organe bearbeiten Personendaten von Einwohnerinnen und Einwohnern im Rahmen ihrer öffentlichen Aufgabe gemäss ihrem gesetzlichen Auftrag. Entsprechend halten sich öffentliche Organe an die verfassungsmässigen Prinzipien bei Grundrechtseingriffen.

Das Legalitätsprinzip bestimmt, dass Personendaten nur dann bearbeitet werden dürfen, wenn dies in einer rechtlichen Grundlage vorgesehen ist. Zudem verlangt die Bundesverfassung, dass die Datenbearbeitung im öffentlichen Interesse liegt und dass sie für die Aufgabenerfüllung geeignet, erforderlich und damit verhältnismässig ist.

In diesem Umfeld besteht für Einwilligungen kein Raum. Ein öffentliches Spital kann die Behandlung von Patientinnen und Patienten nicht davon abhängig machen, dass diese dazu einwilligen, ihre Patientendokumentation in einer Cloud zu speichern, die nicht datenschutzkonform ist. Die Gesundheitsversorgung muss für alle gewährleistet sein.

Auch die Berechnung von tiefen Risiken hilft nicht, wenn es um die Anwendung einer ausländischen Bestimmung geht, mit der völkerrechtliche Verfahrensgrundsätze umgangen werden sollen. Beispielsweise verpflichtet der US CLOUD Act US-amerikanische Unternehmen dazu, den Behörden Zugriff auf ihre Kundendaten zu geben, auch wenn diese ausserhalb des Landes gespeichert sind. Aber Grundrechte können nicht ausgehebelt werden, indem die Rechtsverletzung zu einer Compliance-Frage erklärt wird.

Für öffentliche Organe gelten die verfassungsmässigen Vorgaben, die nicht durch die Privatautonomie des Privatrechts ersetzt werden können. Trotzdem schleichen sich privatrechtliche Argumentationen immer mehr in den öffentlichen Bereich ein – dort gehören sie nicht hin.

Öffnung der Spitalumgebung führt zu hohen Risiken
(https://www.datenschutz.ch/tb/2023/oeffnung-der-spitalumgebung-fuehrt-zu-hohen-risiken)

Besondere Risiken für die Grundrechte: M365
(https://www.datenschutz.ch/tb/2023/besondere-risiken-fuer-die-grundrechte-m365)

Die digitale Transformation schreitet voran

Öffentliche Organe wollen Cloud-Lösungen einsetzen und später soll die Künstliche Intelligenz (KI) als Unterstützung beigezogen werden. In beiden Fällen handelt es sich um eine Auslagerung der Datenbearbeitung durch das öffentliche Organ. Bei beiden finden Datenbearbeitungen statt, bei denen die datenschutzrechtlichen Vorgaben Anwendung finden. Der gesetzliche Rahmen für Auslagerungen ist klar definiert.

Die Datenschutzbeauftragte unterstützt die öffentlichen Organe bei der Erreichung der Digitalisierungsziele effizient und wirksam. Sie hat im Berichtsjahr für die öffentlichen Organe weiter präzisiert, was die rechtlichen Vorgaben für konkrete Fallkonstellationen bedeuten. Der Verhältnismässigkeitsgrundsatz verpflichtet die öffentlichen Organe, Alternativen zu prüfen für die Produkte, die für die Aufgabenerfüllung beigezogen werden sollen. Das Datenschutzrecht ist eine wertvolle Leitplanke auf dem Weg zur digitalen Transformation.

Präzisierungen in einem komplexen Umfeld
(https://www.datenschutz.ch/tb/2023/praezisierungen-in-einem-komplexen-umfeld)

Dabei ist die Datenschutzbeauftragte früh einzubeziehen, denn bei Projekten der digitalen Transformation erreichen die Datenbearbeitungen neue Dimensionen.

Datenschutz und Informationssicherheit sind keine neue Herausforderung

Im September 2023 trat das totalrevidierte Datenschutzgesetz des Bundes (DSG) in Kraft. Die Datenschutzbeauftragte erhielt zahlreiche Anfragen von öffentlichen Organen im Kanton Zürich. Sie wollten wissen, was sie für die Umsetzung des neuen Gesetzes zu unternehmen haben. Die Datenschutzbeauftragte klärte unter anderem in Aus- und Weiterbildungsveranstaltungen sowie mit einem Merkblatt über die Anwendbarkeit der verschiedenen Datenschutzgesetze auf.

Das Datenschutzgesetz des Bundes gilt für Bundesorgane und Private. Für öffentliche Organe der Kantone gilt das jeweilige kantonale Datenschutzgesetz. Nur in Spezialfällen fallen öffentliche Organe im Kanton unter die Bestimmungen des DSGs. Umgekehrt kann das kantonale Datenschutzrecht allerdings auch für Private gelten.

Die Anfragen zeigten aber auf, dass das Datenschutzrecht noch wenig bekannt ist. Dies, obwohl es seit bald 30 Jahren in Kraft ist. Auch die steigende Anzahl der Meldungen von Datenschutzvorfällen zeigt, dass noch grosser Nachholbedarf besteht bei der Umsetzung von datenschutzrechtlichen Vorgaben sowie von Massnahmen im Bereich der Informationssicherheit.

Öffentliche Organe unterstehen dem IDG – aber nicht immer
(https://www.datenschutz.ch/tb/2023/oeffentliche-organe-unterstehen-dem-idg-aber-nicht-immer)

Private unterstehen dem DSG – aber nicht immer ausschliesslich
(https://www.datenschutz.ch/tb/2023/private-unterstehen-dem-dsg-aber-nicht-immer-ausschliesslich)

Falsche Stammdaten führen zu Datenschutzvorfällen
(https://www.datenschutz.ch/tb/2023/falsche-stammdaten-fuehren-zu-datenschutzvorfaellen)

Kontrollen als wirksames Instrument

Eine der Hauptaufgaben der Datenschutzbeauftragten ist die Durchführung von Kontrollen bei öffentlichen Organen. Sie überprüft dabei, ob die datenschutzrechtli-

chen und technischen Vorgaben eingehalten werden. Im Jahr 2023 wurden erstmals 60 Kontrollen durchgeführt. Neben den Datenschutzreviews mit Selbstdeklaration bei Gemeinden hat die Datenschutzbeauftragte Schwerpunkte im Gesundheits- und Bildungsbereich gesetzt. Die Kontrollen stellen ein wirksames Instrument dar.

Die Datenschutzbeauftragte stellt bei Kontrollen Mängel fest und unterstützt die kontrollierten öffentlichen Organe bei der Umsetzung von erforderlichen Massnahmen. So können der Datenschutz und die Informationssicherheit bei öffentlichen Organen im Kanton Zürich wirksam verbessert werden.

Informationssicherheit flächendeckend fördern *(https://www.datenschutz.ch/tb/2023/informationssicherheit-flaechendeckend-foerdern)*

Datenschutzprobleme in Alters- und Pflegezentren *(https://www.datenschutz.ch/tb/2023/datenschutzprobleme-in-alters-und-pflegezentren)*

Die Bevölkerung muss vertrauen können

Das Vertrauen der Bevölkerung ist für die Aufgabenerfüllung der öffentlichen Organe essenziell. Die Cyberangriffe machen auch vor der staatlichen Infrastruktur nicht halt. Auch die Nachrichten über misslungene IT-Projekte stellen das Vertrauen in Frage. Die digitale Transformation birgt grosse Chancen. Gleichzeitig wächst jedoch die Komplexität, was neue, zusätzliche Risiken mit sich bringt.

Die Bevölkerung muss gerade in diesem Umfeld der rasanten Entwicklungen auf die grundrechtskonforme Umsetzung des Datenschutzes durch die öffentlichen Organe vertrauen können. Die Vorgaben sind rechtlich, aber auch technisch umzusetzen. Dabei ist die Datenschutzbeauftragte früh einzubeziehen, denn bei Projekten der digitalen Transformation erreichen die Datenbearbeitungen neue Dimensionen. Das Datenschutzrecht ist hier eine grosse Hilfe, damit die digitale Transformation auch nachhaltig gelingt.

Das Datenschutzrecht ist anwendbar *(https://www.datenschutz.ch/tb/2023/das-datenschutzrecht-ist-anwendbar-2)*

Datenschutz und Sicherheit – wird jetzt alles gut? *(https://www.datenschutz.ch/tb/2023/aus-und-weiterbildung)*

Mehr Kontrollen, mehr Websitezugriffe

Die für das Jahr 2023 festgelegten Indikatoren der Datenschutzbeauftragten zeigen eine stabile Entwicklung. Die Anzahl durchgeführter Kontrollen stieg stark an.

Kontrollen

Die Datenschutzbeauftragte verfolgt als Entwicklungsschwerpunkt, dass regelmässig und nachhaltig Kontrollen der Datenbearbeitungen gewährleistet sind. Nach pandemiebedingten Beschränkungen der Kontrolltätigkeit hat diese bereits im Jahr 2022 zugenommen und erreichte im Jahr 2023 die im Indikator vorgesehene Anzahl von 60 Kontrollen pro Jahr. Kontrollen verlaufen über einen längeren Zeitraum und zeichnen sich erst mit deren Abschluss im Indikator ab, womit dies im Berichtsjahr der Fall war. Neben Datenschutzreviews mit Selbstdeklaration bei Gemeinden wurden Schwerpunkte im Gesundheits- und Bildungsbereich gesetzt.

Anzahl Kontrollen

KEF	2021	2022	2023
60	22	24	60

Beratung und Vorabkontrollen

Ein weiterer Entwicklungsschwerpunkt zielt ab auf die effiziente und wirksame Unterstützung der Verwaltung, um die Digitalisierungsziele zu erreichen. Sowohl die Beratungstätigkeit der Datenschutzbeauftragten wie auch die durchgeführten Vorabkontrollen betrafen vordergründig komplexe Digitalisierungsprojekte. Die Anzahl stieg im üblichen Rahmen leicht an.

Anzahl Beratungen

KEF	2021	2022	2023
750	753	569	793

Aus- und Weiterbildung

Die Aus- und Weiterbildungstätigkeit der Datenschutzbeauftragten konnte auf hohem Niveau stabil weitergeführt werden. Es besteht weiterhin grosser Bedarf, sich Wissen anzueignen zu datenschutzrechtlichen Themen wie auch zu Fragen der Informationssicherheit.

Anzahl Aus- und Weiterbildungen

KEF	2021	2022	2023
20	29	29	27

Websitezugriffe

Die Zugriffe auf die Website www.datenschutz.ch sind stark gestiegen. Die Website umfasst einen umfangreichen Schatz an konkreten Hilfestellungen. Die Datenschutzbeauftragte verweist in den Aus- und Weiterbildungsveranstaltungen und in den Beratungen konsequent auf die Online-Informationen. Weiter führte die erstmalig vollkommen digitale Veröffentlichung des Tätigkeitsberichts zu zusätzlichen Websitebesuchen. Besonders grosse Aufmerksamkeit genoss im Jahr 2023 auch die neu lancierte Lernplattform lerne.datenschutz.ch *(https://lerne.datenschutz.ch/)*.

Anzahl Websitezugriffe

KEF	2021	2022	2023
45 000	39 225	49 585	74 567

IDG-Revision auf der Zielgeraden

Das Gesetz über die Information und den Datenschutz wird totalrevidiert. Die Vorlage wurde vom Regierungsrat verabschiedet und befindet sich in der Beratung beim Kantonsrat. Die Datenschutzbeauftragte begrüsst die Revision.

Im Sommer 2023 hat der Regierungsrat die Totalrevision des Gesetzes über die Information und den Datenschutz (IDG) zuhanden des Kantonsrates verabschiedet, nachdem im Sommer 2022 die Vernehmlassung durchgeführt wurde und die Eingaben im Gesetzestext eingearbeitet wurden. Die Datenschutzbeauftragte war seit der Initiierung der Totalrevision im Jahr 2020 in der Arbeitsgruppe zur Erarbeitung des Entwurfs zum neuen IDG sowie im Steuerungsausschuss vertreten. Zurzeit berät die Kommission für Staat und Gemeinden des Kantonsrats die Vorlage.

Mit der Totalrevision des IDG wird das Öffentlichkeitsprinzip gestärkt und die Transparenz erhöht. Es wird eine Beauftragte oder ein Beauftragter für das Öffentlichkeitsprinzip eingeführt. Die Datenschutzbeauftragte soll mit dieser Aufgabe betraut werden. Gemeinden haben damit zukünftig auch eine Stelle, die sie zu Fragen des Öffentlichkeitsprinzips konsultieren können. Es wird eine Regelung zu offenen Behördendaten aufgenommen, um einem breiteren Publikum gewisse Daten zur Nutzung zur Verfügung zu stellen. Öffentliche Organe sollen im Bereich der Künstlichen Intelligenz verpflichtet werden, ein öffentlich zugängliches Verzeichnis zu führen, das die von ihm verwendeten algorithmischen Entscheidsysteme auflistet. Zudem wird eine Grundlage geschaffen, um Pilotversuche zu ermöglichen. Unter strengen Voraussetzungen können vor dem Erlass einer Rechtsgrundlage mittels einer Verordnung besondere Personendaten im Rahmen eines Pilotversuchs bearbeitet werden.

Bei der Einarbeitung der Eingaben in die aktuelle Vorlage wurden wichtige Punkte der Datenschutzbeauftragten berücksichtigt und umgesetzt. So lässt die aktuelle Vorlage die Amtshilfe nur noch in Einzelfällen zu. Die Bestimmung entspricht wieder der geltenden Gesetzgebung und wurde konkretisiert. Sie soll im Einzelfall den Austausch von Informationen zwischen öffentlichen Organen ermöglichen, wenn diese die Informationen benötigen und nachweisen können, dass sie zur Bearbeitung berechtigt sind. Ausserdem wurden auch weitere materielle und formelle Anmerkungen der Datenschutzbeauftragten umgesetzt.

Nach der Vernehmlassung fanden jedoch auch neue Regelungen Einzug in die Vorlage. Zu gewissen Neuerungen hat die Datenschutzbeauftragte im Nachgang Stellung genommen und ihre Einschätzung der Kommission präsentiert.

Die Datenschutzbeauftragte begrüsst die verabschiedete Vorlage im Grundsatz. Bei den drei nachfolgenden Themen besteht für die Datenschutzbeauftragte noch Diskussionsbedarf.

Die Vorlage zum IDG sieht neu vor, dass die Datenschutzbeauftragte die Empfehlungen und Beurteilungen im Tätigkeitsbericht den öffentlichen Organen zur schriftlichen Stellungnahme vorzulegen hat. Diese Stellungnahmen sollen dem Tätigkeitsbericht angefügt werden. Diese Bestimmung bedeutet einen Eingriff in die Unabhängigkeit der Datenschutzbeauftragten und ist damit nicht kompatibel mit den übergeordneten europarechtlichen Vorgaben. Bereits heute berichtet die Datenschutzbeauftragte in ihren Tätigkeitsberichten nur über abgeschlossene Fälle, bei denen die öffentlichen Organe genügend Raum für Stellungnahmen haben.

Weiter enthält die IDG-Vorlage neue Bestimmungen, die den Informationszugang im Rahmen des Öffentlichkeitsprinzips pauschal einschränken. Protokolle von nicht öffentlichen Sitzungen, bei Exekutiven auch die Anträge, Mitberichte und Stellungnahmen sollen in jedem Fall generell unter Verschluss bleiben. Das bestehende IDG wie auch die Gesetzesvorlage sehen eine Interessenabwägung vor, die Einschränkungen des Informationszugangs ermöglicht, wenn öffentliche Interessen der Bekanntgabe entgegenstehen. Das Grundrecht auf Zugang zu amtlichen Dokumenten ist Teil der Kantonsverfassung. Damit es nicht unzulässig eingeschränkt wird, ist bei der bewährten bisherigen Regelung der Interessenabwägung zu verbleiben.

Schliesslich stellt sich die Frage, ob das Öffentlichkeitsprinzip durch ein formelles Schlichtungsverfahren ergänzt werden soll, wie dies der Bund und andere Kantone kennen. Die Gesetzesvorlage sieht keine Aufsichtsbehörde im Bereich des Öffentlichkeitsprinzips vor. Mit der Einführung eines Schlichtungsverfahrens könnten Streitfälle zwischen betroffenen Personen und öffentlichen Organen beigelegt werden, ohne dass die ordentlichen Gerichte bemüht werden müssten. Damit würde allen beteiligten Personen und Institutionen eine effiziente und vertrauenswürdige Vorgehensweise angeboten.

Die Rolle der Datenschutzbeauftragten

Die Datenschutzbeauftragte ist mit Beratungen und durch Vorabkontrollen in eine Vielzahl einzelner Digitalisierungsprojekte involviert. Sie teilt ihre Expertise im Bereich Datenschutz und gestaltet so die Digitalisierung mit. Immer wichtiger wird ihre Mitarbeit auf der strategischen Ebene, um den Schutz der Grundrechte von Anfang an in die digitale Transformation zu verankern.

Digitalisierung besteht nicht nur aus vielen einzelnen IKT-Projekten. Mit der Digitalisierung geht eine eigentliche Verwaltungsreform einher. Digitalisierung ist eine breit angelegte Strategie und braucht neben dem Fokus auf die einzelnen Projekte einen Blick für das grosse Ganze.

Strategische Initiativen und strategische Inputs

Die Strategie des Regierungsrats zur digitalen Verwaltung fasst die Leitsätze im Slogan «gemeinsam digital unterwegs» zusammen. Die Umsetzung der Leitsätze erfolgt durch strategische Initiativen. Sie gehen die digitale Transformation der kantonalen Verwaltung direktionsübergreifend und ganzheitlich an. Die fünf strategischen Initiativen decken folgende Bereiche ab: Leistungen, Organisation, Infrastruktur, Daten und Recht. Der Leitsatz «gemeinsam» der Digitalisierungsstrategie impliziert auch Zusammenarbeit mit der Datenschutzbeauftragten. Sie soll in die Arbeit der strategischen Initiativen einbezogen werden. Werden heute strategische Weichen gestellt, die dem Datenschutz nicht gerecht werden, führt dies in Zukunft zu aufwendigen und teuren Anpassungen. Die Digitalisierung kann nur mit Datenschutz gelingen. Für den Einbezug der Datenschutzbeauftragten in die Arbeit der strategischen Initiativen braucht es neue Gefässe. So sind strategische Inputs der Datenschutzbeauftragen möglich, die über die Beratung und Vorabkontrollen einzelner Projekte hinausgehen.

Kann die Datenschutzbeauftragte bereits auf der strategischen Ebene ihre Inputs zu den Anforderungen für KI einbringen, schafft dies Planungssicherheit für die Projekte.

Mehrwert der Mitarbeit beim Legal Hub

Mit der strategischen Initiative Recht bestehen schon Kontakte. Wichtig ist die Mitarbeit der Datenschutzbeauftragen beim Legal Hub, dem rechtlichen Kompetenzzentrum für die digitale Transformation. Dort werden die rechtlichen Grundlagen für die Digitalisierung erarbeitet. Dazu gehört beispielsweise der Umgang mit künstlicher Intelligenz (KI). KI-Projekte enthalten meist Datenbearbeitungen mit besonderen Risken für die Grundrechte. Sie sind der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten. Kann die Datenschutzbeauftragte bereits auf der strategischen Ebene ihre Inputs zu den Anforderungen für KI einbringen, schafft das Planungssicherheit für die Projekte. Werden die Anforderungen für KI von Anfang an im Projekt umgesetzt, können negative Befunde der Datenschutzbeauftragten in der Vorabkontrolle verhindert und dadurch aufwendige Anpassungen vermieden werden.

Offen für weiteren Austausch

Auch mit den vier anderen strategischen Initiativen bestehen Kontakte. In jedem Bereich sind die Bedürfnisse für Inputs der Datenschutzbeauftragten unterschiedlich. Die Datenschutzbeauftragte kontrolliert auch die Informationssicherheit. Sie wird deshalb gerade bei der strategischen Initiative Infrastruktur eine wichtige Rolle spielen.

Zusammenarbeit bei spezifischen Digitalisierungsprojekten

Die Zusammenarbeit bei spezifischen Digitalisierungsprojekten bleibt wichtig. Drei Beispiele zeigen verschiedene Arten, wie die Datenschutzbeauftragte ihre Rolle wahrnimmt: erstens die begleitende Beratung beim Zürikonto *(https://www.datenschutz.ch/tb/2023/begleitende-beratung-beim-zuerikonto)*, zweitens die anstehende Vorabkontrolle für das elektronisches Bewilligungsverfahren im Gesundheitswesen *(https://www.datenschutz.ch/tb/2023/bewilligungen-im-gesundheitswesen-vereinfachen)* und drittens eine Intervention bei der Eigentumsabfrage zu Grundstücken auf dem GIS-Browser *(https://www.datenschutz.ch/tb/2023/grundbuchdaten-im-internet)* aufgrund vieler Anfragen von Bürgerinnen und Bürgern.

Begleitende Beratung beim Zürikonto

Mit dem Zürikonto will der Kanton für seine Kundinnen und Kunden einen zentralen Einstiegspunkt für den Bezug digitaler Leistungen der Verwaltung schaffen. Langfristig sollen die Leistungen der drei Ebenen Bund, Kanton und Gemeinde zusammengeführt und somit soll eine einfache Nutzung der Verwaltungsdienstleistungen ermöglicht werden.

Die Datenschutzbeauftragte wirkt beim Projekt Zürikonto seit 2021 im Rahmen einer begleitenden Beratung mit. Dazu gehörten auch drei Gesetzgebungsprojekte, zu denen die Datenschutzbeauftragte regelmässig Inputs gab.

Login-Lösungen im dynamischen Umfeld

Ein zentraler Punkt des Zürikontos ist die Gestaltung des Logins. Anfang 2021 lehnte das Schweizer Stimmvolk das erste E-ID-Gesetz ab. Entsprechend brauchte es neue Ideen für das Login, die den Datenschutz berücksichtigen, die Ansprüche an die Informationssicherheit erfüllen und rechtlich abgestützt sind. Eine Arbeitsgruppe unter Einbezug der Datenschutzbeauftragten machte sich Gedanken über eine eigene E-ID im Kanton Zürich. Schliesslich wurde der Kanton Zürich als Pilotkanton für das Behörden-Login AGOV des Bundes gewählt. AGOV wird ab 2024 den Zugang zum Zürikonto ermöglichen und ist künftig mit der E-ID des Bundes kompatibel.

Für die Datenbearbeitung im Zürikonto setzte die Datenschutzbeauftragte auf eine konsequente Umsetzung des Grundsatzes der Datensparsamkeit.

Datensparsamkeit statt Persönlichkeitsprofile

Beim Zürikonto verlangte die Datenschutzbeauftragte eine konsequente Umsetzung des Grundsatzes der Datensparsamkeit. Das Zürikonto ist als Portal konzipiert und somit ein Ort des Absprungs zu den entsprechenden Dienstleistungen. Die Datenschutzbeauftragte wies darauf hin, dass im Zürikonto keine Informationen zu den verschiedenen Geschäften der Kundinnen und Kunden vorhanden sein dürfen. Ansonsten würden hier detaillierte Persönlichkeitsprofile über eine Vielzahl von Personen entstehen.

Rechtsgrundlagen schaffen

Die Datenschutzbeauftragte machte darauf aufmerksam, dass für das Zürikonto neue Rechtsgrundlagen geschaffen werden müssen. Sie begleitete drei Gesetzgebungsprojekte und gab regelmässig Inputs für eine detaillierte Regelung der Datenbearbeitung. Zuerst wurde mit dem Projekt Digilex das Verwaltungsrechtspflegegesetz für elektronische Verfahrenshandlungen angepasst (LS 175.2 *(http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=175.2)*). Danach wurde eine ausführende Verordnung über elektronische Verfahrenshandlungen im Verwaltungsverfahren verfasst. Schliesslich folgte der Entwurf für ein neues Gesetz über digitale Basisdienstleistungen. Damit werden die Anforderungen an die Normstufe erfüllt,

denn wichtige Bestimmungen und schwere Eingriffe in die Grundrechte müssen in einem formellen Gesetz festgehalten sein, das durch den Kantonsrat beraten und angenommen wird. Das Zürikonto zeigt beispielhaft, wie grosse Digitalisierungsprojekte mit Rechtsetzungsprojekten einhergehen können.

Bewilligungen im Gesundheitswesen vereinfachen

Mit dem elektronischen Bewilligungsverfahren Gesundheitswesen (eBeGe), sollen einzelne Anträge zusammengeführt werden. Das vereinfacht das Verfahren. So werden jedoch sämtliche, auch sehr heikle Personendaten an einer Stelle zusammengeführt. Daraus entstehen Persönlichkeitsprofile.

Ob eine Ärztin mit Berufskolleginnen oder -kollegen eine Privatklinik eröffnen, ein Chiropraktiker im eigenen Namen und auf eigene Rechnung auf Hausbesuche gehen oder eine Akupunkteurin Behandlungen in einer eigenen Praxis anbieten will – der Weg in die selbstständige Berufstätigkeit ist in der Gesundheitsbranche kompliziert und von Unsicherheiten geprägt.

Viele Bewilligungen von vielen Stellen

Ist die Berufsausübungsbewilligung der Gesundheitsdirektion erlangt, braucht es eine Vertretungs- und Assistenzbewilligung, damit Hilfspersonen angestellt werden können. Möchte eine Gesundheitsfachperson ihre Praxis als Unternehmen organisieren, benötigt sie eine Betriebsbewilligung, Bewilligungen für den Umgang mit Heil- und Betäubungsmitteln und allenfalls Spezialbewilligungen, etwa für die Behandlung von Suchtpatientinnen und -patienten oder zur Anwendung von Fortpflanzungsverfahren. Die Anforderungen sind umfangreich, nach Bereich unterschiedlich und die Grundlagen sowohl in kantonalen als auch in eidgenössischen Erlassen geregelt. Die Bewilligungen werden durch die Gesundheitsdirektion, die kantonale Heilmittelkontrolle, den Kantonsärztlichen Dienst oder die Abteilung für Gesundheitsberufe und Bewilligungen ausgestellt.

Das Verfahren wird so vereinfacht. Doch werden in Zukunft sämtliche, auch sehr heikle Personendaten an einer Stelle konzentriert.

Viele heikle Personendaten

Die betroffenen Personen müssen beispielsweise einen Strafregisterauszug einreichen. Zudem beantragt die Gesundheitsdirektion beim Bundesamt für Justiz die Ausstellung eines Sonderprivatauszugs. Dieser wird der betroffenen Person zugestellt, die ihn der Gesundheitsdirektion zur Vervollständigung der Antragsunterlagen übermittelt. Im Sonderprivatauszug sind auch Strafurteile aufgeführt, die im regulären Auszug nicht aufgeführt sind. Weiter sind Daten zur Berufsausübung offenzulegen, wie die eingeschränkte Zulassung zum Medizinalberuf oder bereits entzogene Bewilligungen. Diese Daten werden zudem bei Datenbekanntgaben an andere öffentliche Organe oder juristische Personen des Privatrechts mitgeteilt, beispielsweise zur Organisation des Notfalldienstes im Kanton.

Der Regierungsrat stellte mit der Strategie Digitale Verwaltung 2018–2023 die Weichen für die digitale Zukunft der kantonalen Verwaltung. Im Hauptprojekt eBeGe sollen die einzelnen Anträge zusammengeführt werden. Das Verfahren wird so vereinfacht. Die antragstellenden Personen geben bei diesen Bewilligungsverfahren allerdings tiefe Einblicke in ihr Leben. In Zukunft werden nun sämtliche, auch sehr heikle Personendaten an einer Stelle konzentriert. Daraus entsteht ein Persönlich-

keitsprofil, in das die Gesundheitsdirektion und die ihr unterstehenden öffentlichen Organe Einsicht erhalten.

Persönlichkeitsprofile verlangen hohen Schutz

Die Datenschutzbeauftragte beriet die Gesundheitsdirektion und zeigte die Risiken auf, die eine Digitalisierung des Prozesses mit sich bringt. Persönlichkeitsprofile zeichnen ein sehr umfassendes Bild einer Person. Deshalb müssen öffentliche Organe einen hohen Schutz vor Missbrauch gewährleisten können. Die Datenschutzbeauftragte unterstützte die Gesundheitsdirektion bei der Eruierung der Risiken im Zusammenhang mit dem Missbrauch solcher besonderer Personendaten sowie bei der Erstellung der Datenschutz-Folgenabschätzung und des ISDS-Konzepts. In einem nächsten Schritt wird die Datenschutzbeauftragte anhand des ISDS-Konzepts der Gesundheitsdirektion die notwendigen technischen und organisatorischen Massnahmen überprüfen.

Automatische Passkontrolle am Flughafen Zürich überzeugt

Beim E-Gate-System am Flughafen Zürich wertet eine Kamera das Gesicht der Person biometrisch aus, gleicht danach diese Daten mit den Informationen im Reisepass ab und überprüft verschiedene polizeiliche Datenbanken auf eventuelle Einträge. Die Datenschutzbeauftragte kontrollierte das E-Gate-System am Flughafen Zürich. Das System wird von der Kantonspolizei Zürich betrieben und erlaubt eine vollständig automatisierte Passkontrolle für Reisende.

Die Datenschutzbeauftragte überprüfte die Bereiche Recht, Organisation und Technik umfassend. Sie stützt sich bei Kontrollen auf die vorgelegten Unterlagen des öffentlichen Organs wie auch auf Interviews und Stichproben vor Ort. Rechtlich wurde abgeklärt, ob sich jede Bearbeitung von Personendaten auf eine genügende rechtliche Grundlage stützt, die durch das E-Gate-System vorgenommen wird. Dann wurde überprüft, ob Aufbewahrungsfristen für Personendaten definiert sind und auch eingehalten werden.

Die Kontrolle zeigte, dass die Prozesse im Bereich Datenschutz und Informationssicherheit vorbildlich definiert sind und auch eingehalten werden.

Zur Kontrolle gehörte auch eine Prüfung der Verträge mit Dritten auf die Vorgaben des Datenschutzes und der Informationssicherheit, wenn diese potenziell Zugang zu Personendaten haben. Organisatorisch und technisch wurden unter anderem das Informationssicherheits- und Datenschutzkonzept, die Betriebsorganisation, das Rollen- und Berechtigungskonzept und die Regelung der Authentifizierung für das System überprüft.

Die Kontrolle zeigte, dass die Prozesse im Bereich Datenschutz und Informationssicherheit vorbildlich definiert sind und auch eingehalten werden. Im gesamten Prozess wird das Prinzip der Datensparsamkeit berücksichtigt. Die Daten werden umfassend verschlüsselt. Die technischen Dokumentationen sind vollständig. Mängel wurden lediglich in untergeordneten Punkten ausgemacht. So stellte die Datenschutzbeauftragte fest, dass einzelne Fehlerreports des Systems nicht gelöscht wurden. Sie forderte zudem Verbesserungen beim Schwachstellenmanagement.

Grundbuchdaten im Internet

Bisher physische oder nur beschränkt zugängliche Register werden im Internet abrufbar. Das vereinfacht den Zugang von Bürgerinnen und Bürgern zu staatlichen Informationen, ein wichtiges Ziel der Digitalisierung der Verwaltung. Werden dabei Personendaten veröffentlicht, stellen sich besondere datenschutzrechtliche Fragen.

Das Internet unterscheidet sich in der Art des Zugangs und in der Anzahl der Adressatinnen und Adressaten von gedruckten Publikationen: Informationen im Internet sind weltweit und jederzeit abrufbar. Sie können beliebig verwendet und vielfältig kombiniert werden und sie sind auf unbefristete Zeit zu finden, weil ihre weitere Speicherung und Verbreitung nicht beeinflusst werden kann. Betroffene Personen können eine Publikation im Internet weder berichtigen noch nachführen oder löschen. Einträge zu einem Namen lassen sich mit einer Suchmaschine einfach finden. Zudem können Personendaten ungehindert in Länder ohne gleichwertiges Datenschutzniveau fliessen. Bei einer Veröffentlichung von Personendaten im Internet besteht also ein erhöhtes Risiko für Persönlichkeitsverletzungen. Diese Überlegungen gelten auch für die Veröffentlichung von Grundbuchdaten im Internet.

Bei einer Veröffentlichung von Personendaten im Internet besteht ein erhöhtes Risiko für Persönlichkeitsverletzungen.

Seit Ende August 2023 ist es im Kanton Zürich möglich, die Daten des Grundbuchs digital über das Geografische Informationssystem des Kantons, den kantonalen GIS-Browser, abzufragen. Zur Verfügung gestellt werden der Name oder die Firma der Eigentümerin oder des Eigentümers, die zuletzt bekannte Wohnadresse sowie die Eigentumsform.

Keine Datensperre möglich

Die Datenschutzbeauftragte erhielt sofort nach dem Aufschalten des Diensts zahlreiche Anfragen von Privaten. Die Zulässigkeit dieser Datenbekanntgabe wurde in Frage gestellt. Zudem wurde nach der Möglichkeit einer Datensperre durch Betroffene gefragt. Laut Schweizerischem Zivilgesetzbuch ist jede Person berechtigt, ohne Interessennachweis Auskunft über die Bezeichnung des Grundstücks und die Grundstücksbeschreibung, den Namen und die Identifikation der Eigentümerin oder des Eigentümers und die Eigentumsform sowie das Erwerbsdatum zu erhalten. Die Grundbuchverordnung des Bundes erlaubt es den Kantonen, diese Daten elektronisch zugänglich zu machen. Die Daten dürfen nur grundstücksbezogen abgerufen werden und die Auskunftssysteme müssen vor Serienabfragen geschützt sein. Damit sollen die Risiken der Veröffentlichung im Internet eingeschränkt werden.

Mit der kantonalen Grundbuchverordnung hat der Kanton Zürich die nötige Rechtsgrundlage für die elektronische Veröffentlichung geschaffen. Weder das eidgenössische noch das kantonale Grundbuchrecht sehen eine Möglichkeit vor, die Bekanntgabe dieser Daten sperren zu lassen. Auch eine Sperre gemäss § 22 des IDG ist nicht möglich. Diese Bestimmung erlaubt lediglich die Sperre von nicht öffentlichen Daten, die von einem öffentlichen Organ aufgrund spezialgesetzlicher Ermächtigung voraussetzungslos bekannt gegeben werden dürfen. Dies ist beispielsweise bei

Adressauskünften aus dem Einwohnerregister der Fall. Bei Datenbekanntgaben aus dem Grundbuch besteht kein Sperrrecht.

Datenschutzvorfall trotz Schutzmassnahmen

Bei Inbetriebnahme des Systems waren die Abfrage pro IP-Adresse und Tag sowie die Gesamtzahl der Abfragen pro Tag beschränkt. Abfragen waren nur mit IP-Adressen aus der Schweiz möglich und die Web Application Firewall (WAF) verfügte über eine Regel, die DDOS-Attacken erkennt und blockiert. Damit sollten die Schutzbestimmungen aus der Grundbuchverordnung umgesetzt werden. Generell soll verhindert werden, dass das Grundbuch kopiert und durch Dritte nachgebildet wird.

Das Notariatsinspektorat meldete der Datenschutzbeauftragten kurz nach der Lancierung der Online-Abfrage einen Datenschutzvorfall. Erste Auswertungen zeigten eine Konzentration von Abfragen auf einzelne Gemeinden an einem Tag, die sich am nächsten Tag auf andere Gemeinden verschob. Das Notariatsinspektorat ergriff Sofortmassnahmen, um eine widerrechtliche Verwendung des Systems auszuschliessen. Die Tageslimite und die Limite pro IP-Adresse wurden herabgesetzt und später mit einer Stundenlimite und einer Tageslimite pro Gemeinde ergänzt.

Die Datenschutzbeauftragte schlug in Zusammenarbeit mit den Verantwortlichen des Notariatsinspektorats und des Amts für Raumentwicklung (ARE) zusätzliche Massnahmen vor. Dazu gehören die Prüfung einer Registrierungspflicht und die Aufnahme der Mobiltelefonnummer der Benutzerinnen und Benutzer.

Besondere Risiken für die Grundrechte: M365

Öffentliche Organe dürfen nur Personendaten bearbeiten, wenn dies notwendig ist, um die gesetzlichen Aufgaben zu erfüllen. Dabei sind sie an die Grundrechte gebunden. Jede Bearbeitung von Personendaten ist ein Eingriff in die Grundrechte. Bevor Cloud-Dienste eingesetzt werden können, muss ein öffentliches Organ deshalb nicht nur abklären, ob diese Bearbeitung der Personendaten einer gesetzlichen Aufgabe dient, sondern auch, ob der Eingriff in die Grundrechte verhältnismässig ist.

Bei allen Cloud-Lösungen gelten die gleichen datenschutzrechtlichen Vorgaben. So dürfen keine gesetzlichen Schweigepflichten entgegenstehen, etwa das Arztgeheimnis oder das Steuergeheimnis. Zudem bleibt das öffentliche Organ immer für seine Personendaten verantwortlich, auch wenn die Bearbeitung in die Cloud ausgelagert wird. Es muss also sicherstellen, dass auch in diesem Fall der Datenschutz gewährleistet ist.

CLOUD Act und das Völkerrecht

Viele Cloud-Anbieter sind US-amerikanische Unternehmen. Sie fallen unter den Clarifying Lawful Overseas Use of Data Act, kurz CLOUD Act. US-Behörden können diese Unternehmen dazu verpflichten, Personendaten herauszugeben, auch wenn diese Daten ausserhalb der USA gespeichert sind. Dadurch werden die Bestimmungen der internationalen Rechtshilfe umgangen, die Teil des Völkerrechts ausmachen. Der Rechtshilfeweg ist zudem ein wesentlicher Eckpfeiler des Schweizer Rechtsstaats. Seine Umgehung verstösst gegen den Ordre public.

Das Netzwerk Egovpartner berät Gemeinden und Städte bei der Digitalisierung. Es liess untersuchen, ob und wie öffentliche Organe im Kanton Zürich M365 des US-amerikanischen Unternehmens Microsoft grundrechtskonform einsetzen können.

Die Gutachter Professor Dr. iur. Markus Schefer, Staatsrechtsprofessor der Universität Basel, und Dr. iur. Philip Glass, Lehrbeauftragter der Universität Basel, kommen zum Schluss, dass die Speicherung von Personendaten durch M365 in der Cloud einen schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Die Daten sämtlicher Personen im Zuständigkeitsbereich des öffentlichen Organs werden durch den Einsatz dieser Cloud-Lösung auf Vorrat zugänglich für US-Behörden. Das öffentliche Organ verliert die Kontrolle über die Daten. Es kann den Anspruch auf Schutz der Betroffenen vor Missbrauch ihrer persönlichen Daten, wie er in der Bundesverfassung festgelegt ist, nicht mehr sicherstellen.

Die Gutachter schreiben, die Situation werde dadurch erschwert, dass keine Alternativen zu M365 geprüft werden. Es entstehe eine Abhängigkeit der schweizerischen Behörden von Microsoft. Weiter wiesen die Gutachter Egovpartner darauf hin, dass kein ausreichender rechtlicher Rahmen bestünde, der für eine Auslagerung in die Cloud eines US-Unternehmens ausreichen würde.

Diese Einschätzungen decken sich mit denjenigen der Datenschutzbeauftragten.

Die Daten sämtlicher Personen im Zuständigkeitsbereich des öffentlichen Organs werden durch den Einsatz dieser Cloud-Lösung auf Vorrat zugänglich für US-Behörden.

Eine Rechtsgrundlage für digitale Basisdienste schaffen

Die Staatskanzlei erarbeitete einen Entwurf für die Rechtsgrundlagen von digitalen Basisdiensten des Kantons. Das Gesetz über digitale Basisdienste (DigiBasis) soll Regelungen enthalten zur elektronischen Identifikation, zum elektronischen Webzugang des Kantons Zürikonto sowie zum digitalen Arbeitsplatz der Mitarbeitenden von öffentlichen Organen im Kanton Zürich.

Die Datenschutzbeauftragte wurde im Rahmen der Arbeiten am Entwurf von DigiBasis konsultiert und konnte vorab wichtige Punkte zum Datenschutz einbringen. Sie wies früh auf die Notwendigkeit zur Regelung der Rahmenbedingungen für die Auslagerung der Datenbearbeitungen beim digitalen Arbeitsplatz in die Cloud von US-amerikanischen Unternehmen hin. Dazu gehört beispielsweise, dass eine Auslagerung der Bearbeitung von besonderen Personendaten in die Microsoft Cloud nicht möglich ist, solange das Unternehmen Zugriff auf die Daten nehmen kann.

Diese Regelung muss für sämtliche öffentlichen Organe im Kanton Zürich gelten, also nicht nur für die kantonale Verwaltung und die Gemeinden, sondern etwa auch für die Hochschulen oder die Spitäler. Diese und weitere Punkte brachte die Datenschutzbeauftragte auch in ihrer Vernehmlassungsantwort zu DigiBasis ein.

M365 bei Gemeinden

Im Jahr 2023 legten verschiedene Gemeinde- und Stadtverwaltungen ihr Projekt zur Einführung von M365 der Datenschutzbeauftragten zur Vorabkontrolle vor. Sie zeigte auf, dass die Verwendung einer Cloud immer eine Auslagerung einer Bearbeitung ist. Bei allfälligen Grundrechtsverletzungen bleiben die Gemeinden verantwortlich.

Durch die Nutzung von M365 erhält Microsoft Einsicht in diese Personendaten und muss sie auf Anordnung einer US-Behörde bekannt geben, da das US-Unternehmen dem CLOUD Act untersteht. Gemeinden und ihre Mitarbeitenden bearbeiten besondere Personendaten sowie solche, die unter gesetzlichen Geheimnispflichten stehen, wie das Steuer- oder Sozialhilfegeheimnis. Wenn diese mit M365 in der Cloud bearbeitet werden, besteht eine besondere Gefährdung der Grundrechte.

Eine Liste von Sozialhilfeempfängerinnen und -empfängern darf deshalb nur in der Excel-Cloud-Variante geführt werden, wenn die Personendaten verschlüsselt werden und das Schlüsselmanagement bei den Gemeinden bleibt. Dasselbe gilt, wenn eine Steuerveranlagungsverfügung in Microsoft Exchange Online abgelegt werden soll.

Die Datenschutzbeauftragte informierte die Gemeinden auch über die Verwendung der Rahmenverträge der Schweizerischen Informatikkonferenz (SIK) mit Microsoft. Der Rahmenvertrag kann allerdings nur ab 250 Nutzerinnen und Nutzern eingesetzt werden.

Öffnung der Spitalumgebung führt zu hohen Risiken

Der Alltag im Spital ist für das Personal geprägt von Zeitknappheit und hoher Verantwortung. Oft müssen lebensentscheidende Massnahmen innerhalb von wenigen Sekunden getroffen werden. Spitäler gelangten im Jahr 2023 an die Datenschutzbeauftragte mit Fragen zur datenschutzkonformen Einführung von M365. Jedoch sind im Gesundheitsbereich auch Produkte anderer Anbieter begehrt.

Die Spitalinfrastruktur wird durch den Einsatz der Cloud schlanker. Anstatt ein spitaleigenes System von zahlreichen Mitarbeitenden programmieren und unterhalten zu lassen, werden diese Unterstützungsprozesse an den Cloud-Anbieter ausgelagert. Das Spital kann sich dann auf den Betrieb des Klinikinformationssystems (KIS) konzentrieren. Mit Cloud-Software können Dienstleistungen patientenfreundlicher gestaltet werden. Konsultationen können per Videokonferenzen angeboten werden oder über Apps können Patientinnen und Patienten direkt Unterlagen hochladen oder Termine vereinbaren. Für die Wartung und die Pflege solcher Clouds müssen ihre Betreiber Zugriff auf die Anwendung haben und bekommen dadurch Einblick in die vorhandenen Personendaten. Diese Öffnung der Spitalumgebung für Dritte führt zu hohen datenschutzrechtlichen Risiken.

Viele besondere Personendaten, viele Daten unter Geheimnispflichten

Gesundheitsdaten sind immer besondere Personendaten. Personendaten von Patientinnen und Patienten verlangen nach einem hohen Schutz. Das ergibt sich aus der besonderen Natur des Behandlungsverhältnisses. Allerdings kann auch ein Röntgenbild ohne Namensanschrift aufgrund der Einzigartigkeit eindeutig einer Person zugeordnet werden. Die Adresse auf einem Brief mit dem Generalsekretariat des Spitals als Absender mag noch nicht als besonderes Personendatum gelten. Geht aus dem Absender hervor, dass eine Person von einer Ärztin aus der Onkologie angeschrieben wurde, dann handelt es sich hier aber um besondere Personendaten. Aus dem Absender können Rückschlüsse auf den Gesundheitszustand der Person gemacht werden. Zusätzlich unterstehen Ärztinnen und Ärzte sowie ihre Hilfspersonen der beruflichen Schweigepflicht (Art. 321 Schweizerisches Strafgesetzbuch, StGB, SR 311.0 *(https://www.fedlex.admin.ch/eli/cc/54/757_781_799/de#book_2/tit_18/lvl_u9)* und § 15 Abs. 1 Kantonales Gesundheitsgesetz, GesG, LS 810.1 *(http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=810.1)*). Bereits der Umstand, dass ein Behandlungsverhältnis zwischen einem Patienten und einer Ärztin besteht, fällt unter die Geheimnispflicht.

Bei Informationen, die der gesetzlichen Schweigepflicht unterstehen, und besonderen Personendaten ist die Auslagerung in eine Cloud eines US-Unternehmens ohne zusätzliche Massnahmen nicht datenschutzkonform.

Gesundheitsversorgung kann nicht von Einwilligung abhängig gemacht werden

Das Spital bleibt in jedem Fall verantwortlich für seine Daten. Die datenschutzkonforme Auslagerung in die Cloud gestaltet sich deshalb schwierig. Informationen, die der gesetzlichen Schweigepflicht unterstehen, und besondere Personendaten können ohne zusätzliche Massnahmen nicht datenschutzkonform in eine Cloud eines US-Unternehmens ausgelagert werden. Selbst in die Cloud eines europäischen Unternehmens können Informationen, die der beruflichen Schweigepflicht unterstehen, nicht einfach so ausgelagert werden. Das Offenbaren der Informationen an Dritte stellt eine Straftat dar. Von der Schweigepflicht kann eine Person nur im Einzelfall durch die vorgesetzte Stelle oder die betroffene Person entbunden werden. Spitälern und anderen Gesundheitsinstitutionen wie Spitex- und Pflegeheime, die einen öffentlichen Leistungsauftrag erfüllen, können die Auslagerung nicht mit einer Einwilligung der Patientinnen und Patienten rechtfertigen. Sie müssen die Gesundheitsversorgung der Zürcher Bevölkerung gewährleisten. Die Gesundheitsversorgung kann nicht von der Einwilligung einer Person zur Bearbeitung von Personendaten in der Cloud abhängig gemacht werden.

Präzisierungen in einem komplexen Umfeld

Bevor öffentliche Institutionen Daten durch Dritte bearbeiten lassen, müssen viele Fragen geklärt werden. Das öffentliche Organ ist verantwortlich dafür, dass die Vorgaben im Zusammenhang mit der Auslagerung eingehalten werden.

Die Datenschutzbeauftragte stellt auf ihrer Website ausführliche Unterlagen zur Verfügung, um die öffentlichen Organe in ihren Digitalisierungsvorhaben zu unterstützen.

Viele Gemeinden planen im Rahmen ihrer Digitalisierungsstrategie den Einsatz von M365. Mit der Nutzung dieser Dienstleistungen von Microsoft werden Daten in einer Cloud bearbeitet. Dies stellt eine Auslagerung dar. Zudem untersteht das amerikanische Unternehmen dem CLOUD Act *(https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_microsoft365_gemeinden.pdf)* der USA. Die Datenschutzbeauftragte hat einen Leitfaden *(https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_microsoft365_gemeinden.pdf)* erstellt, mit dem die Gemeinden Schritt für Schritt die datenschutzrechtlich notwendigen Punkte für die Nutzung von M365-Applikationen prüfen können.

Die Nutzung einer Cloud stellt eine Auslagerung dar.

Das Schlüsselmanagement ist zentral

Der Leitfaden bringt Klarheit über die Anforderungen und die Möglichkeiten bei der Auslagerung von besonderen Personendaten sowie von Daten unter besonderen Amtsgeheimnissen oder dem Berufsgeheimnis im Anwendungsbereich des CLOUD Act. Diese Daten sind so zu verschlüsseln, dass der Anbieter keinen Zugang zu den Daten erhält ohne das Zutun der Gemeinde. Der Schlüssel muss also bei der Gemeinde liegen.

Bei der Erstellung des Leitfadens stand die Datenschutzbeauftragte im engen Austausch mit Egovpartner, der eigenständigen Zusammenarbeitsorganisation von Gemeinden, Städten und dem Kanton Zürich. Sie stand auch im Kontakt mit Microsoft. Sie erläuterte den Vertreterinnen und Vertretern des Unternehmens die gesetzlichen Vorgaben, die die Gemeinden einhalten müssen. Zudem erklärte sie die Anforderungen an die Verschlüsselung von Daten, die in den Anwendungsbereich des CLOUD Act fallen.

Die Komplexität der einzelnen Digitalisierungsprojekte nimmt ständig zu. Die Datenschutzbeauftragte unterstützt öffentliche Organe im Rahmen ihrer Beratungstätigkeit bei Fragen. Sie überarbeitet zudem ihre Publikationen regelmässig. Nach der Veröffentlichung des Leitfadens für Gemeinden wird auch der Leitfaden für den Einsatz von M365 im Bildungsbereich überarbeitet. Darin wird der Umgang mit besonderen Personendaten und Berufsgeheimnissen präzisiert.

Termin-Apps und Schliesssysteme

Cloud-Lösungen werden für die unterschiedlichsten Zwecke eingesetzt. Oft wird bei ihrem Einsatz nicht wahrgenommen, dass besondere Personendaten bearbeitet werden.

Termin-App

Eine Gruppe psychiatrischer Kliniken wollte eine App einführen, über die Patientinnen und Patienten auf ihre Termine zugreifen können. Auf der Plattform werden Namen, Geburtsdatum, Geschlecht, Wohnadresse, Telefonnummer, E-Mail-Adresse, Ein- und Austrittsdatum, behandelnde Ärztinnen und Ärzte, Pflegedauer, Station, Zimmernummer und Termininformationen gespeichert. Informationen zu Befunden und Behandlung sind auf der Cloud-App nicht gespeichert.

In ihrer Vorabkontrolle machte die Datenschutzbeauftragte darauf aufmerksam, dass die Mitarbeitenden des schweizerischen Cloud-Anbieters, die für den Betrieb und die Wartung Zugang zum System benötigen, klar zu benennen sind. Auf diese Weise können sie als Hilfspersonen qualifiziert werden. Dadurch kann ein strafbares Offenbaren von Berufsgeheimnissen vermieden werden.

Ein Schliesssystem in der Cloud

Eine Gemeinde beabsichtigte die Einführung eines neues Türschliesssystems für die Verwaltung, ihre Geschäftsstellen und die Schulen. Sie entschied sich für ein Schliesssystem, das vollständig auf einer externen Cloud betrieben wird. Die Schliessanlage ist vollständig elektronisch. So können Zugangsberechtigungen einfach vergeben, aber auch wieder entzogen werden. Dadurch bleiben die Anlagen auch bei Schlüsselverlusten sicher.

Die Datenschutzbeauftragte wies darauf hin, dass bei solchen Schliesssystemen das Verhalten der Personen in der Cloud gespeichert wird. Daraus können Bewegungsprofile entstehen, die als besondere Personendaten gelten. Sie sind mit zusätzlichen Massnahmen zu schützen.

Automatisierte Überwachung von Fahrverboten

Eine Gemeindepolizei möchte bei einem signalisierten Fahrverbot eine Videoüberwachung einsetzen. Das System soll fehlbare Fahrzeuglenkerinnen und -lenker automatisch erkennen und direkt büssen.

Die Gemeindepolizei fragte die Datenschutzbeauftragte, ob die Polizeiverordnung ausreiche für den Einsatz eines solchen Systems. Die Videoüberwachung wird zur Strafverfolgung eingesetzt. Die Datenschutzbeauftragte beurteilte den Eingriff in die Grundrechte der betroffenen Personen durch den Einsatz des vorgeschlagenen Systems als schwer. Diese Überwachung muss in einem formellen Gesetz vorgesehen sein und mit Rahmenbedingungen versehen werden. Eine Verordnung reicht nicht aus.

Solche Überwachungssysteme können nur als verhältnismässig beurteilt werden, wenn eine gesteigerte Notwendigkeit vorliegt.

Das Bundesgericht urteilte zu ähnlichen Fragen im Bereich der automatisierten Fahrzeugfahndung und Verkehrsüberwachung (BGer 1C_39/2021 und BGE 146 I 11). Bei der Normstufe verlangt es ein formelles Gesetz für solche Systeme. Bei der Normdichte müssen mindestens der Zweck der Überwachung, die bearbeiteten Personendaten und ihre Aufbewahrungsdauer geregelt sein.

Solche Überwachungssysteme können nur als verhältnismässig beurteilt werden, wenn eine gesteigerte Notwendigkeit vorliegt und andere Massnahmen versagt haben. Eine gesteigerte Notwendigkeit besteht beispielsweise bei einer starken Nachtruhestörung in einem städtischen Wohnquartier aufgrund der Missachtung des Fahrverbots oder einer starken Wildruhestörung aufgrund einer Missachtung des Fahrverbots in einem Wald.

Auch wenn eine gesteigerte Notwendigkeit besteht, dürfen durch die Überwachung nur die Personendaten bearbeitet werden, die zur Aufgabenerfüllung notwendig sind. Bei der Videoüberwachung eines Fahrverbotes heisst das, dass ausschliesslich das Kennzeichen des Fahrzeugs erfasst werden darf. Die Fahrzeuglenkerinnen und -lenker oder vorbeigehende Passantinnen und Passanten dürfen nicht erkennbar sein. Der Überwachungszeitraum muss auf das notwendige Minimum beschränkt werden. Die Videokameras dürfen also nur während des Zeitraums in Betrieb sein, in dem das Fahrverbot gilt.

Einsicht in eine Videoaufnahme des Kinderhorts

Ein Kind kam mit einem zerrissenen T-Shirt nach Hause. Es erzählte den Eltern von einem Vorfall zwischen ihm und der Hortmitarbeiterin, der zur zerrissenen Kleidung geführt habe. Die Eltern wissen, dass der Aussenbereich des Kinderhorts videoüberwacht wird. Sie stellten ein Gesuch zur Einsicht in die Videoaufnahmen, damit sie allfällige rechtliche und strafrechtliche Schritte gegen die Hortmitarbeiterin einleiten können.

Die Gemeindeschreiberin wandte sich mit der Anfrage der Eltern an die Datenschutzbeauftragte. Die Beauftragte erläuterte der Gemeindeschreiberin das Zugangsrecht zu den eigenen Personendaten. Das Recht auf Zugang zu den eigenen Personendaten kann eingeschränkt werden, wenn überwiegende öffentliche oder private Interessen der Bekanntgabe entgegenstehen.

Ein Videoüberwachungsreglement muss auch den Ablauf und die zuständige Stelle benennen, damit betroffene Personen ihre Rechte wahrnehmen können.

Die Videoaufnahmen umfassen Personendaten einer Drittperson, nämlich der Hortmitarbeiterin. Hier muss abgewogen werden, ob die Interessen der Hortmitarbeiterin daran, dass die Videoaufnahmen nicht herausgegeben werden, das Recht und das Interesse des Kindes am Zugang zu den eigenen Personendaten überwiegen.

Das Videoüberwachungsreglement der betroffenen Gemeinde legte nicht konkret fest, wer zuständig ist für die Bearbeitung von Gesuchen zur Einsicht in Videoaufnahmen. Die Gemeindeschreiberin wird aber als zugriffsberechtigte Person im Reglement genannt. Deshalb kann sie zur Bearbeitung des Gesuchs die Aufnahmen einsehen.

Der Leitfaden Videoüberwachung durch öffentliche Organe *(https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_videoueberwachung_durch_oeffentliche_organe.pdf)* der Datenschutzbeauftragten zeigt die notwendigen Elemente eines Reglements zur Videoüberwachung auf. Dazu gehört auch, dass der Ablauf und die zuständige Stelle benannt sein müssen, damit betroffene Personen ihre Rechte wahrnehmen können.

Das Datenschutzrecht ist anwendbar

2023 ist das Jahr, in dem Online-KI-Generatoren wie ChatGPT für die breite Bevölkerung zugänglich wurden. Auch die öffentlichen Organe wollen die neue Technologie einsetzen. Das kantonale Recht regelt den Einsatz von KI (noch) nicht spezifisch. Beim Einsatz von KI werden aber oft Personendaten bearbeitet. Deshalb sind die Regeln des Datenschutzes anwendbar.

Chatbots bearbeiten Informationen über die Personen, die Fragen stellen. Werden Steuerdossiers von einer KI vorsortiert, sind Informationen von Steuerzahlerinnen und Steuerzahlern betroffen. Das Datenschutzrecht gilt unabhängig von der Technologie und gibt Grundsätze und Prozesse vor. Sie müssen angesichts der Entwicklung von KI neu betrachtet werden. Exemplarisch kann dies an der Gesetzmässigkeit und der Transparenz illustriert werden.

Rechtsgrundlagen bei zusätzlichen Risiken für die Grundrechte

Das kantonale Datenschutzrecht erlaubt die Bearbeitung von Personendaten, wenn dies zur Erfüllung von gesetzlichen Aufgaben geeignet und erforderlich ist. Die gesetzliche Aufgabe des öffentlichen Organs kann den Einsatz von KI rechtfertigen. Entsteht jedoch aufgrund des Einsatzes von KI ein zusätzliches Risiko für die Grundrechte, ist ein rechtlicher Rahmen zu schaffen, der diesen Risiken Rechnung trägt. Würden beispielsweise Entscheidungen auf der Basis einer KI-generierten Einschätzung getroffen, könnten zusätzliche Risiken bei der Profilbildung, bei der Richtigkeit der Daten oder bei diskriminierenden Resultaten liegen.

Das IDG definiert den Einsatz neuer Technologien wie KI als besonderes Risiko für die Grundrechte.

Transparenz über den Einsatz von KI

Transparenz ist ein Grundsatz im Datenschutz. Die betroffenen Personen sollen wissen, wie ihre Daten bearbeitet werden. Dieser Grundsatz ist aufgrund der Entwicklungen im Bereich KI neu zu bewerten. Wie kann Transparenz über den Einsatz von KI gewährleistet werden? Der aktuell im Kantonsrat diskutierte Entwurf des Gesetzes über die Information und den Datenschutz (IDG) sieht ein Verzeichnis vor, worin die öffentlichen Organe die verwendeten algorithmischen Entscheidsysteme auflisten müssen, wenn sie sich auf die Grundrechte von Personen auswirken. Das ist eine allgemeine Massnahme zur Transparenz über den Einsatz von KI. Weiter ist zu regeln, dass betroffene Personen über eine Entscheidung zu informieren sind, die ausschliesslich auf einer automatisierten Bearbeitung von Personendaten beruht und mit Rechtsfolgen versehen ist oder sie erheblich beeinträchtigt. Zudem ist vorzusehen, dass betroffene Personen ihren Standpunkt darlegen dürfen und eine Überprüfung der automatisierten Entscheidung durch eine natürliche Person verlangen können.

Generelle Pflicht zur Vorabkontrolle

Wenn öffentliche Organe ein neues Projekt starten, das Personendaten beinhaltet, müssen sie eine Datenschutz-Folgenabschätzung (DSFA) erstellen. Zeigt die DSFA besondere Risiken für die Grundrechte, muss das Projekt der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden. Das IDG definiert den Einsatz neuer Technologien wie KI als besonderes Risiko für die Grundrechte. Somit besteht für alle KI-Projekte die Pflicht zur Vorabkontrolle durch die Datenschutzbeauftragte.

Einsatz von KI in Schulen

Schülerinnen und Schüler können mit KI-Generatoren den Umgang mit Künstlicher Intelligenz als Unterrichtsmittel erlernen. Lehrpersonen oder weitere Angestellte können diese Technologie bei der Ausübung ihres Berufs als Arbeitsmittel nutzen. Bei der Nutzung von KI-Generatoren werden regelmässig Personendaten bearbeitet. Personendaten bleiben schützenswert, auch wenn sie öffentlich zugänglich und etwa auf Websites veröffentlicht sind.

Bei den Anfragen aus dem Bildungsbereich zu Microsoft-Produkten stand der Umgang mit künstlicher Intelligenz im Fokus. Die Datenschutzbeauftragte hat zum Gebrauch von sogenannten Power Apps beraten, die Microsoft Copilot benutzen. Diese KI-Generatoren ermöglichen umfangreiche Recherchen und Abklärungen. Zudem können sie grammatikalisch korrekte sowie stilsichere Zusammenfassungen formulieren. Dafür werden einfache Fragen als Texte eingegeben, wonach wissenschaftliche Ausgabetexte oder Grafiken generiert werden.

Die Nutzung von KI-Generatoren durch Schülerinnen und Schüler muss separat von der Nutzung durch Lehrpersonen und andere Mitarbeitende von Schulen beurteilt werden. Im Bereich der gesetzlichen Grundlage und der Informationsverwaltung ergeben sich Unterschiede.

Dazu kommt, dass in Schulen Personendaten bearbeitet werden, die Kinder betreffen. Schon die Verwendung eines KI-Generators zur Erstellung von Texten durch eine Schülerin oder einen Schüler ist ein Personendatum – meistens bereits aufgrund der Verknüpfung mit den Nutzerdaten. Es können aber auch Personendaten in den Texten selbst vorhanden sein, die dann mit dem KI-Generator bearbeitet werden.

Aus der Art und der Häufigkeit der Nutzung sowie den abgefragten Inhalten kann ein Persönlichkeitsprofil eines Schulkindes entstehen.

Schulen können KI-Generatoren zur Bearbeitung von Personendaten verwenden, wenn dafür eine rechtliche Grundlage vorliegt. Der Bildungsauftrag kann die Verwendung des KI-Generators als Unterrichtsmittel rechtfertigen. Die Schule bleibt in jedem Fall verantwortlich für die Datenbearbeitung. Aus Transparenzgründen sind die Erziehungsberechtigten über den Einsatz von KI-Generatoren und die damit verbundenen Datenbearbeitungen zu informieren.

Biometrische Daten und Persönlichkeitsprofile der Kinder

Gewisse KI-Tools beruhen auf der technischen Analyse von Handschriften oder Stimmerkennungen. Dies sind biometrische Daten und damit besondere Personendaten. Aus der Art und der Häufigkeit der Nutzung sowie den abgefragten Inhalten kann ein Persönlichkeitsprofil eines Schulkindes entstehen. Auch Persönlichkeitsprofile sind besondere Personendaten. Die Bearbeitung besonderer Personendaten bedeutet eine hohe Gefährdung für die Grundrechte der betroffenen Person. Deshalb sind höhere Schutzvorkehrungen notwendig.

Die Verwendung eines KI-Generators stellt eine neue Datenbearbeitung unter Verwendung neuer Technologien dar. Die Datenschutzbeauftragte wies auf die Pflicht der Schulen hin, vor dem Einsatz von neuen Technologien Datenschutz-Folgenabschätzungen zu erstellen. Darin sollen die Risiken der Datenbearbeitungen bestimmt und technische sowie organisatorische Massnahmen zur Minderung der Gefahren definiert werden. Aufgrund des Schulumfelds kann eine Vielzahl von Personen betroffen sein. Solche Projekte müssen der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden.

Idealerweise können Schulen die bearbeiteten Personendaten anonymisieren, bevor Anbieterinnen und Anbieter von KI-Dienstleistungen sie einsehen und für eigene Zwecke nutzen können.

Online-KI-Generatoren bearbeiten Personendaten

Die Datenschutzbeauftragte beantwortete im Jahr 2023 häufig Fragen zum Einsatz von Online-KI-Generatoren. Sie bearbeiten Personendaten über die Nutzerinnen und Nutzer. Zudem können auch Personendaten in den Prompts vorkommen.

Online-KI-Generatoren wie ChatGPT werden normalerweise von Dritten betrieben. Ihr Einsatz ist deshalb eine Auslagerung beziehungsweise eine Datenbearbeitung im Auftrag. Datenschutzrechtliche Probleme liegen etwa vor, wenn Anbieter von Online-KI-Generatoren Personendaten des öffentlichen Organs verwenden, oder bei der Erfüllung der vertraglichen Anforderungen. Zu den vertraglichen Anforderungen gehören das geltende Recht, der Gerichtsstand sowie die Zweckbindung. Auch der Anbieter der Plattform darf die Daten ausschliesslich für die Zwecke verwenden, die durch die gesetzlichen Aufgaben des auftraggebenden öffentlichen Organs erlaubt sind.

Bei der Beratung weist die Datenschutzbeauftragte darauf hin, dass die Informationen von Online-KI-Generatoren nicht notwendigerweise richtig sind, da sie auf Wahrscheinlichkeitsrechnungen basieren. Die Richtigkeit der bearbeiteten Daten ist jedoch ein Grundsatz des Datenschutzes.

Zu den vertraglichen Anforderungen gehören das geltende Recht, der Gerichtsstand sowie die Zweckbindung.

Merkblatt zur Nutzung von Online-KI-Generatoren

Die Staatskanzlei hat für die kantonale Verwaltung ein Merkblatt zur Nutzung von Online-KI-Generatoren publiziert. Die Datenschutzbeauftragte lieferte Inputs. Das Merkblatt definiert, wie ein sehr reduzierter Einsatz von Online-KI-Generatoren für öffentliche Organe möglich ist.

Die Online-KI-Generatoren sind kein behördliches Arbeitsmittel. So dürfen keine behördlichen Personendaten und keine Informationen zum öffentlichen Organ in den Prompts verwendet werden. Diese und weitere Anforderungen schränken zwar die Verwendung von Online-KI-Generatoren stark ein, trotzdem können sie für zahlreiche Aufgaben verwendet werden. Sie können beispielsweise genutzt werden für Zusammenfassungen von öffentlich zugänglichen Informationen, Brainstormings zu allgemeinen Themen oder als Formulierungshilfe für allgemeine Texte.

Experimente zum erweiterten Einsatz von Online-KI-Generatoren

Bereits gibt es Experimente für einen weitergehenden Einsatz von Online-KI-Generatoren. Die Datenschutzbeauftragte beriet öffentliche Organe im Schulbereich, die eine anonymisierte Nutzung von Online-KI-Generatoren ermöglichen wollen. Ebenso haben sich Gemeinden bei der Datenschutzbeauftragten gemeldet. Sie wollen angepasste KI-Generatoren einsetzen, um ihre öffentlich verfügbaren Informationen personalisiert zugänglich zu machen.

Die Datenschutzbeauftragte als Partnerin beim KI-Einsatz

Die Datenschutzbeauftragte folgt den technologischen Entwicklungen und lässt Erkenntnisse sofort in ihre Beratung einfliessen. Sie ist eine Partnerin für die öffentlichen Organe bei der Digitalisierung und hilft beim datenschutzkonformen Einsatz von KI.

Falsche Stammdaten führen zu Datenschutzvorfällen

In Zürcher Spitälern gibt es pro Jahr mehrere Hunderttausend Ein- und Austritte von Patientinnen und Patienten. Dabei passieren Fehler, die oft zu Datenschutzvorfällen führen. Diese müssen der Datenschutzbeauftragten gemeldet werden. Aufgrund der Meldungen der letzten Jahre kann sie nun einige Massnahmen empfehlen, mit denen Datenschutzvorfälle verhindert werden können.

Im vergangenen Jahr gab es 72 Meldungen zu Datenschutzvorfällen, wodurch die Grundrechte der betroffenen Personen gefährdet wurden. In 39 Fällen wurden Personendaten per E-Mail oder Brief an unberechtigte Personen verschickt. Oft stammten die Meldungen von Spitälern. Spitäler bearbeiten sehr viele besondere Personendaten von einer grossen Anzahl Personen. Zudem stehen diese Daten unter einem Berufsgeheimnis.

Die Ursachen für die Datenschutzvorfälle in Spitälern sind vielfältig. So stehen die Mitarbeitenden am Empfang oft unter Zeitdruck. Zudem gibt es beim Spitalpersonal eine hohe Fluktuation. Die neuen Mitarbeitenden sind deshalb immer wieder unvertrauten Situationen ausgesetzt. Die fehlende oder mangelhaft umgesetzte Digitalisierung ist ein weiterer Grund. Die Patientinnen und Patienten tragen ihre Namen und Adressen meist handschriftlich auf einem Formular ein. Das Formular wird dann abgetippt und die Informationen werden so ins Klinikinformationssystem übertragen. Dabei passieren Fehler, weil die Patientinnen und Patienten unleserlich schreiben, selbst einen Schreibfehler machen oder die Mitarbeitenden sich vertippen. All diese Ursachen führen zu falschen Stammdaten wie Namen, Adresse, Telefonnummer und E-Mail. Daraus folgt, dass das Spital regelmässig medizinische Daten wie Arztberichte an falsche Personen verschickt.

Die fehlende oder mangelhaft umgesetzte Digitalisierung ist oft ein Grund für Datenschutzvorfälle.

Alle Meldungen von Datenschutzvorfällen werden durch die Datenschutzbeauftragte abgeklärt. Mit den folgenden Massnahmen können Spitäler, aber auch andere Einrichtungen Fehler in Stammdaten vermindern.

- **Liste führen:** Öffentliche Organe sollten Datenschutzvorfälle zentral aufzeichnen und klassifizieren. Die Vorfälle können danach klassifiziert werden, wie schwer die Datenschutzverletzung war, welche Abteilung betroffen war und bei welchem Prozess der Vorfall geschehen ist, beispielsweise beim Verschicken des Sprechstundenberichts oder des Formulars zur Patientenanmeldung. So können Muster erkannt und gezielte Massnahmen umgesetzt werden.
- **Schulungen und Sensibilisierungen:** Spitäler bearbeiten viele besondere Personendaten. Deshalb können auch viele Fehler passieren, die die Grundrechte der betroffenen Personen gefährden. In diesem Umfeld sind Mitarbeitende gezielt zu schulen, besonders auch diejenigen am Empfang. Konkrete Vorfälle aus der Spitalpraxis bieten eine ideale Grundlage für diese Schulungen. Abteilungen mit hoher Fluktuation und vielen temporären Arbeitskräften sind häufiger zu schulen. In den Schulungen können zusammen mit den Mitarbeitenden zusätzliche Massnahmen entwickelt werden. Die Mitarbeitenden wissen oft am besten, wo und warum die Fehler passieren und wie sie verhindert werden können.

- **Double-Opt-in:** Bei Anmeldungen für Newsletter oder bei Internetportalen ist das Double-Opt-in üblich. Beim Double-Opt-in werden den Nutzenden ihre Angaben in einem E-Mail zugesandt. Das Konto wird erst eröffnet, wenn der Erhalt des E-Mails bestätigt wird. Die Plattformbetreibenden sind dann sicher, dass die E-Mail-Adresse richtig ist. In einem Spital könnte das Double-Opt-in so umgesetzt werden: Die Patientin oder der Patient füllt das Eintrittsformular aus. Die oder der Spitalmitarbeitende überträgt den Inhalt in ein System, das die Daten der Person an die angegebene E-Mail-Adresse schickt. Erst nachdem die Person den Erhalt des E-Mails bestätigt hat, werden die Angaben ins Klinikinformationssystem integriert.
- **Plattform:** Informationen können auch über eine Plattform mit den Patientinnen und Patienten ausgetauscht werden, statt sie per E-Mail oder Post zu senden. Ein Spital könnte dafür den Patientinnen und Patienten beim Eintritt die persönlichen Zugangsdaten geben.
- **Vier-Augen-Prinzip:** Beim Einpacken von Berichten in Couverts kann das Vier-Augen-Prinzip sinnvoll sein. Dies ist jedoch aufwendig und durch die Routine kann die Wirkung abnehmen.
- **Rundschreiben:** Sind sehr viele Stammdaten fehlerhaft, dann ist das Anschreiben jeder einzelnen Person die einzige Möglichkeit, die Fehler zu korrigieren. Diese Massnahme ist zwar äusserst aufwendig, aber sehr wirkungsvoll.

Datenschutzprobleme in Alters- und Pflegezentren

In Alters- und Pflegezentren steht der Mensch im Zentrum und nicht der Computer. Sie bearbeiten aber auch viele Gesundheitsdaten. Bei diesen besonderen Personendaten muss dem Datenschutz und der Informationssicherheit ein hoher Stellenwert zukommen. Die Datenschutzbeauftragte führte im Jahr 2023 Kontrollen in 16 Einrichtungen durch. Dabei zeigten sich Mängel, die von fehlenden Plänen zur Abwehr von Hackerangriffen bis hin zu Servern reichten, die öffentlich erreichbar waren.

Im Kanton Zürich gibt es über 300 Alters- und Pflegezentren. Für rund 160 ist die Datenschutzbeauftragte zuständig. In diesen Einrichtungen wohnen über 10 000 Menschen. Die Zentren bearbeiten eine Fülle an Daten, vor allem auch besondere Personendaten über die Bewohnenden, wie Arztberichte, die Dosierung von Medikamenten oder auch Sturzprotokolle. Um den 24-Stunden-Betrieb sicherzustellen, beschäftigen die Alterszentren viele Mitarbeitende. Zudem ist die Fluktuation in der Belegschaft sehr hoch. Diese Voraussetzungen erhöhen die Risiken im Bereich des Datenschutzes und der Informationssicherheit.

Die Datenschutzbeauftragte stellte für ihre Kontrolltätigkeit eine Stichprobe an Alters- und Pflegezentren zusammen. Sie wählte grosse und kleine Zentren sowie solche in Städten und auf dem Land aus, um eine möglichst aussagekräftige Übersicht zu bekommen. Zudem sind die kontrollierten Zentren Stiftungen oder Aktiengesellschaften oder sie machen Teil der Gemeindeverwaltung aus. Einige Organisationen wirtschaften gemeinnützig, andere gewinnorientiert.

Die 10 häufigsten Probleme

- **Unpersönliche Accounts:** In den meisten Alterszentren nutzen die Pflegerinnen und Pfleger gemeinsame Geräte in den Stationszimmern. Oft verwenden sie auch gemeinsame Login-Daten. Veränderungen an Daten wie E-Mails oder Dateien können so nicht nachvollzogen werden. Im schlimmsten Fall löscht beispielsweise ein Pfleger ein wichtiges E-Mail eines Arztes, das für eine andere Pflegerin gedacht war. In einigen Fällen waren die Login-Daten auf die Monitore geklebt. Die unpersönlichen Konten verhindern ein angemessenes Rollen- und Berechtigungskonzept sowie die Kontrolle der Zugriffe.
- **Angreifbare Computer, Server und mobile Geräte:** In Alterszentren werden viele Computer, Server, Tablets und Smartphones eingesetzt. Wenn sie nicht richtig konfiguriert sind, haben es Hacker leicht, auf die gespeicherten Daten zuzugreifen. Die Datenschutzbeauftragte entdeckte viele Fehlkonfigurationen. Bei einem Alterszentrum konnten die Server über das Internet ausgeschaltet werden. Die Orientierung an internationalen Härtungsstandards verhindert, dass Konfigurationen vergessen gehen.
- **Fehlende Updates:** Viele Computer und Handys spielen Updates automatisch ein. Bei den meisten Druckern und anderen Netzwerkgeräten wie Switches und Accesspoints ist dies nicht der Fall. Werden nicht sämtliche Geräte regelmässig aktualisiert und die Versionsstände geprüft, besteht ein Risiko auf Sicherheitslücken. Bei allen kontrollierten Einrichtungen fehlten definierte Prozesse dafür.
- **Fehlende Zwei-Faktor-Authentifizierung:** Beim Online-Banking benutzen alle eine Zwei-Faktor-Authentifizierung. Sie schützt vor vielen Gefahren wie Phishing. Doch nur zwei der kontrollierten Zentren nutzten bei Zugriffen auf Gesundheitsdaten von aussen konsequent eine Zwei-Faktor-Authentifizierung.

- **Keine Konzepte zu Informationssicherheit:** Daten können nur wirkungsvoll geschützt werden, wenn bekannt ist, in welchem System welche Daten gespeichert sind und wofür diese durch wen genutzt werden. Ein Informationssicherheits- und Datenschutz-Managementsystem ermöglicht einen solchen Überblick. Nur wenige Alterszentren verfügen jedoch über ein entsprechendes System. Die Datenschutzbeauftragte stellt öffentlichen Organen umfangreiche Vorlagen für ein Informationssicherheits- und Datenschutz-Managementsystem zur Verfügung.
- **Kein Security Incident Management:** Einige Alterszentren waren schon Ziel von Hackerangriffen. In der aktuellen Bedrohungslage stellt sich nicht die Frage, ob, sondern wann ein Alterszentrum betroffen sein wird. Darum müssen im Voraus klare Verhaltensregeln und Abläufe für solche Fälle festgelegt werden. Alle kontrollierten Zentren waren gut auf Notfälle wie Brand oder Stromausfall vorbereitet. Regeln zum Umgang mit Cybergefahren wie Hackerangriffen fehlten jedoch in allen Notfallhandbüchern.
- **Zu wenig Schulung und Sensibilisierung:** Im medizinischen Bereich, so auch in Alterszentren, werden die Mitarbeitenden regelmässig zu Themen wie Hygiene, neuen Pflegemethoden oder zur Bedienung von Apparaten geschult. Schulungen zum Datenschutz und zur Informationssicherheit gehören jedoch nur in wenigen Alterszentren zum Standard. Regelmässige Schulungen würden den Schutz beispielsweise gegen die althergebrachte, aber immer noch sehr erfolgreiche Angriffstechnik des Phishing sowie gegen Fehlmanipulationen im Umgang mit IKT-Systemen erhöhen.
- **Kein Zugriffsprotokoll Pflegedokumentation:** In Alters- und Pflegezentren müssen alle Pflegerinnen und Pfleger auf alle Informationen von allen Bewohnerinnen und Bewohnern zugreifen können. Sie dürfen jedoch nur Informationen zu Bewohnenden lesen, für die sie auch verantwortlich sind. Vor allem in kleinen Einrichtungen kennen sich die Bewohnenden, die Angehörigen und die Pflegenden oft persönlich. Die Versuchung ist gross, dass eine Pflegerin oder ein Pfleger die Medikamentenliste der Mutter der besten Freundin liest, obwohl sie oder er diese Informationen gar nicht benötigt. Darum müssen Lesezugriffe aufgezeichnet und regelmässig kontrolliert werden. Das war in keinem Alterszentrum der Fall.
- **Backups ohne Verschlüsselung:** Alle Alterszentren verfügen über aktuelle Backups. Diese sind teilweise nicht verschlüsselt. So könnten Dritte auf sämtliche gesicherten Daten zugreifen.
- **Kein Vulnerability-Management:** Die Cyberbedrohungen ändern täglich und Konfigurationsfehler sind schnell passiert. Darum sollte man alle IKT-Systeme regelmässig auf Schwachstellen überprüfen. Das betrifft besonders die Dienstleister der Alterszentren. Mit einem Scanner können Konfigurationsfehler aufgedeckt und Schwachstellen identifiziert werden. Bei zwei Dritteln aller Zentren war kein solcher Scanner im Einsatz.

Informationssicherheit flächendeckend fördern

Heiraten, Baubewilligungen beantragen oder soziale Unterstützung erhalten – Gemeinden und Städte bieten viele Dienstleistungen an. Dafür bearbeiten Gemeinden und Städte Sachdaten, Personendaten, aber auch vertrauliche Dokumente oder besondere Personendaten wie Informationen über Massnahmen der Sozialhilfe. Die Datenschutzbeauftragte konnte bis jetzt in 62 der 160 Gemeinden im Kanton Zürich einen Datenschutzreview mit Selbstdeklaration starten.

Eine Auslagerung der Daten bedeutet nicht auch eine Auslagerung der Verantwortung.

Daten sind mit angemessenen organisatorischen und technischen Massnahmen zu schützen. Um eine nachhaltige Informationssicherheit gewährleisten zu können, müssen Gemeinden und Städte strukturiert vorgehen. Die Grundlage dafür sind Dokumente auf der strategischen, taktischen sowie auf der operativen Ebene. Darin werden die Sicherheitsstrategie definiert, die Informationssicherheitsorganisation aufgebaut sowie das Risiko und der Schutzbedarf der Daten, Anwendungen und Systeme analysiert und beurteilt.

Die Datenschutzbeauftragte unterstützt Gemeinden und Städte beim Aufbau einer nachhaltigen Informationssicherheit. Sie lancierte im Jahr 2021 den Datenschutzreview mit Selbstdeklaration für Gemeinden und Städte. Dafür stellt sie Anleitungen und Vorlagen zur Verfügung. Anhand der Anleitungen können die Gemeinden und Städten die Dokumente selbstständig bearbeiten.

Für die Umsetzung der technischen Schutzmassnahmen wird die Vorlage Technische Richtlinie zur Verfügung gestellt. Sie kann für Gemeinden und Städte genutzt werden, die ihre Daten lokal bearbeiten, wie auch für solche, die sie an einen externen Betreiber ausgelagert haben. Bei einer Auslagerung definiert die Gemeinde oder die Stadt anhand der technischen Richtlinie organisatorische und technische Massnahmen. Diese müssen durch den externen Betreiber umgesetzt werden.

Selbstdeklarationen in 62 Gemeinden und Städten gestartet

Der Kanton Zürich zählt 160 Gemeinden. Seit der Lancierung konnte die Datenschutzbeauftragte den Selbstdeklarationsprozess in 62 Gemeinden und Städten starten. Die Rückmeldungen zeigen, dass die Anleitungen und Vorlagen als hilfreiche Unterstützung bei der Dokumentation und der Umsetzung der organisatorischen und technischen Massnahmen beurteilt wurden. Die Dokumente geben eine Übersicht und ermöglichen damit die Risikobewertung der eingesetzten Geräte, Software und Dienstleister. Zudem sind die Rollen und die Verantwortlichkeiten klar definiert. So ist eine bleibende Grundsicherheit gewährleistet und ein kontinuierlicher Verbesserungsprozess wird angestossen.

Die Datenschutzbeauftragte wird 2024 weitere Gemeinden und Städte in den Prozess der Selbstdeklaration einbinden.

AHV-Nummer der kantonalen Bildungsplanung für Forschungszwecke

Die Bildungsplanung des Kantons verwendet die AHV-Nummern zur Identifikation von Schülerinnen, Schülern und Lehrpersonen für statistische Erhebungen. Sie fragte die Datenschutzbeauftragte an, ob sie diesen Indikator für Forschungsvorhaben weitergeben darf, damit Dritte Informationen verknüpfen können.

Für die Verwendung der AHV-Nummer müssen gewisse technische und organisatorische Massnahmen umgesetzt werden. Zudem muss mit der Zentralen Ausgleichsstelle (ZAS) zusammengearbeitet werden. Personendaten können zur Bearbeitung für nicht personenbezogene Zwecke bekannt gegeben werden, wenn dies nicht durch eine rechtliche Bestimmung ausgeschlossen ist (§ 18 IDG). Im Bereich der Statistik besteht keine solche Bestimmung. Im Gegenteil bestimmt das kantonale Statistikgesetz, dass Personendaten, die im Rahmen von statistischen Tätigkeiten erhoben werden, zu nicht personenbezogenen Zwecken bekannt gegeben werden dürfen.

Ganz unabhängig von der gesetzlichen Grundlage ist in jedem Fall nur die Weitergabe von erforderlichen Personendaten erlaubt. Sonst wäre die Bekanntgabe nicht verhältnismässig. Die AHV-Nummer darf deshalb nur weitergegeben werden, wenn sie absolut notwendig ist, um den Zweck der statistischen Tätigkeit zu erreichen. Wird die Weitergabe als verhältnismässig beurteilt, hat die Empfängerin oder der Empfanger nachzuweisen, dass die Personendaten anonymisiert werden, aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind und die ursprünglichen Personendaten nach der Auswertung vernichtet werden.

Unabhängig von der gesetzlichen Grundlage ist nur die Weitergabe von erforderlichen Personendaten erlaubt.

Was auf die Klassenlisten des Kindergartens gehört

Beim Eintritt in den Kindergarten werden die Kinder einer Klasse zugeteilt. Die Zuteilung erfolgt durch die Schule und wird den Eltern vor Beginn des ersten Kindergartentages mitgeteilt. Eine Schule fragte die Datenschutzbeauftragte an, ob den Eltern eine Klassenliste mit allen Adressen der Kinder bekannt gegeben werden darf. Das würde es den Eltern ermöglichen, sich vor dem ersten Tag mit anderen Eltern abzusprechen oder eine Begleitung für den Weg zum Kindergarten zu organisieren.

Die Datenschutzbeauftragte prüfte eine gesetzliche Grundlage für die regelmässige Bekanntgabe von Klassenlisten. Die Namen der Kinder sowie der Lehrpersonen werden im Rahmen der Bildungs- und Erziehungsaufgaben benötigt, um sich im Unterricht verständigen zu können. Sie dürfen erhoben und unter den Kindern und Lehrpersonen ausgetauscht werden.

Die Ergänzung der Klassenliste mit weiteren Angaben, zum Beispiel der Adresse oder den Namen der Eltern, kann nur erfolgen, wenn die betroffenen Personen einer solchen Datenbekanntgabe im Einzelfall zugestimmt haben. Die Datenschutzbeauftragte wies darauf hin, dass für die Einwilligung die Anmeldungsdokumente des Kindergartens angepasst werden können.

Das Datenschutzlexikon Volksschule *(https://www.datenschutz.ch/lexika/volksschule)* der Datenschutzbeauftragten enthält Antworten zu den meisten Fragen.

Eignung für die Arbeit in Kinder- und Jugendheimen sicherstellen

Seit 2023 müssen Aufsichtsbehörden den Leumund aller Leiterinnen und Leiter sowie von anderen Mitarbeitenden von Kinder- und Jugendheimen, Kinderkrippen und Kinderhorten überprüfen. Dafür holen sie einen Behördenauszug 2 ein. Die Datenschutzbeauftragte klärte ab, welche Informationen an die Verantwortlichen der Institutionen abgegeben werden dürfen.

Der Behördenauszug 2 aus dem Strafregister-Informationssystem VOSTRA enthält mehr Informationen als der Privat- oder der Sonderprivatauszug. Zudem sind die Informationen und die Strafurteile länger ersichtlich als in regulären Auszügen. Die Pflegekinderverordnung (PAVO) verlangt diese Überprüfung aller Leiterinnen und Leiter sowie von anderen Mitarbeitenden von Kinder- und Jugendheimen, Kinderkrippen und Kinderhorten vor der Einstellung. Danach muss sie jährlich wiederholt werden.

Die Datenschutzbeauftragte überprüfte auf Anfrage den Umgang der Aufsichtsbehörde über die Kinder- und Jugendheime des Kantons mit den Informationen aus den Behördenauszügen. Dabei zeigte sich, dass die Behördenauszüge gelöscht werden, sobald sie eingesehen worden sind und die Anstellungsfähigkeit beurteilt wurde. Es wird keine detaillierte Auskunft über den Inhalt der Behördenauszüge erteilt.

Die Datenschutzbeauftragte merkte lediglich an, dass in der Dokumentation zu den Abklärungen zu prüfen ist, wann die Personendaten gelöscht, anonymisiert oder pseudonymisiert werden können. Dafür muss ein entsprechendes Löschkonzept erstellt werden.

Eine detaillierte Auskunft über den Inhalt der Behördenauszüge ist nicht erforderlich und deshalb nicht erlaubt.

Mehrere Gemeinden fragten die Datenschutzbeauftragte, wie sie mit den Informationen des Behördenauszugs 2 umgehen sollen. Gemeinden müssen als Aufsichtsbehörden über Kinderkrippen und Kinderhorte ebenfalls prüfen, ob die Leiterin oder der Leiter sowie die Mitarbeitenden von Kindertagesstätten (Kitas) einen Leumund für ihre Arbeit mit Kindern vorweisen können.

Die Datenschutzbeauftragte beriet die Gemeinden. Bei Einträgen, die dem Kindeswohl entgegenstehen, ist den Verantwortlichen mitzuteilen, dass für eine betroffene Person ein Anstellungshindernis besteht. Damit wird der Zweck der Abklärung erfüllt. Eine weitergehende Auskunft über den Inhalt der Behördenauszüge ist nicht erforderlich und deshalb nicht erlaubt.

Öffentliche Organe unterstehen dem IDG – aber nicht immer

Im Herbst 2023 trat das revidierte Bundesgesetz über den Datenschutz in Kraft. Die Datenschutzbeauftragte erhielt viele Anfragen zur Anwendbarkeit des DSG auf öffentliche Organe. Bei der Bearbeitung von Personendaten ist für die öffentlichen Organe das Gesetz über die Information und den Datenschutz massgebend.

Die Ausnahme für öffentliche Organe

Das DSG ist beispielsweise anwendbar, wenn ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt. Die Aufsicht bleibt aber bei der Datenschutzbeauftragten des Kantons Zürich und richtet sich nach dem IDG. Die Beurteilung, ob ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt, ist nicht immer einfach. Das öffentliche Organ muss in einer Gesamtbetrachtung beurteilen, ob

- mit der Leistung ein öffentliches Interesse verfolgt wird, oder eher ein Interesse, das auch private Personen verfolgen,
- die Tätigkeit überwiegend durch das Privatrecht bestimmt wird,
- für Personal und Finanzen die öffentlich-rechtlichen Bestimmungen gelten oder sich die Organisation nach den privatrechtlichen Bestimmungen richtet,
- das öffentliche Organ in einem Konkurrenzverhältnis zu anderen privaten Anbietern steht.

So kann es sein, dass eine Gemeinde ein Restaurant führt, das in Konkurrenz zu anderen Gastrobetrieben steht. Gleiches gilt für kantonale Spitäler, die ein Restaurant betreiben, das nicht nur für Mitarbeitende zugänglich ist. In beiden Fällen sind für die Personendatenbearbeitungen die Vorgaben des DSG sinngemäss anwendbar.

Die Pflichten öffentlicher Organe im wirtschaftlichen Wettbewerb

Öffentliche Organe, die am wirtschaftlichen Wettbewerb teilnehmen, haben Pflichten gegenüber der Datenschutzbeauftragten. Sie hat dazu ein Merkblatt publiziert. Das öffentliche Organ muss beispielsweise der Datenschutzbeauftragten die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters mitteilen.

Vor einer Datenbekanntgabe ins Ausland hat das Organ die Datenschutzklauseln mitzuteilen, wenn die Bekanntgabe in ein Land ohne einen angemessenen Datenschutz erfolgt und der Datenschutz durch eine vertragliche Vereinbarung gewährleistet werden soll.

Wenn die Datenschutz-Folgenabschätzung einer geplanten Bearbeitung von Personendaten ergibt, dass sie trotz der vorgesehenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, ist das Projekt der Datenschutzbeauftragten zur Stellungnahme vorzulegen. Dieser Schritt ist nicht notwendig, wenn das öffentliche Organ seine Datenschutzberaterin oder seinen Datenschutzberater konsultiert hat.

Stellt das öffentliche Organ eine Verletzung der Datensicherheit fest, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, ist dies der Datenschutzbeauftragten so rasch als möglich zu melden.

Private unterstehen dem DSG – aber nicht immer ausschliesslich

Grundsätzlich ist für Private das Datenschutzgesetz des Bundes (DSG) massgebend. Wenn sie eine kantonale oder kommunale öffentliche Aufgabe erfüllen, dann gilt für diese Privaten im Bereich dieser Aufgabe aber das Gesetz über die Information und den Datenschutz (IDG). Die öffentliche Aufgabe kann durch einen Leistungsvertrag vom Kanton oder der Gemeinde an Private übertragen werden.

Private, die im Rahmen einer Leistungsvereinbarung Sozialpädagogische Familienhilfe (SPF) oder Dienstleistungsangebote in der Familienpflege (DAF) erbringen, unterstehen für diesen Teil dem IDG. In Bezug auf ihre Mitarbeitenden findet hingegen das DSG Anwendung.

Gemeinden können beispielsweise zur Sicherstellung von Krippenplätzen Leistungsvereinbarungen mit privatrechtlich organisierten Kinderkrippen abschliessen. Bearbeitungen von Personendaten im Zusammenhang mit diesen Krippenplätzen unterstehen dem IDG.

Wenn Private eine kantonale oder kommunale öffentliche Aufgabe erfüllen, dann gilt für Tätigkeiten in diesem Bereich das IDG.

Der Elternrat ist ein selbstständig organisiertes Gremium, das die Schule aktiv unterstützt. Er ist aber nicht Teil des öffentlichen Organs Schule. Der Einsatz im Elternrat stellt eine amtliche Tätigkeit dar, wenn die Aktivität eine Grundlage im Organisationsstatut und/oder im Elternratsreglement hat und mit Wissen und Mitwirken der Schule sowie mit Einwilligung der Schulleitung erfolgt. Wenn der Elternrat Personendaten bearbeitet, um die im Organisationsstatut festgelegten öffentlichen Aufgaben zu erfüllen, ist das IDG anwendbar. Alle anderen Datenbearbeitungen fallen unter die Vorgaben des DSG.

Privatspitäler, die auf der kantonalen Spitalliste stehen, unterstehen im Bereich des Leistungsauftrags dem IDG. Alle anderen Aktivitäten fallen unter die Bestimmungen des DSG, etwa in personalrechtlichen Angelegenheiten.

Zahnarztdaten für den Notfalldienst

Die Standesorganisation der Zahnärzte SSO wurde von der Gesundheitsdirektion mit der Organisation des zahnärztlichen Notfalldiensts beauftragt. In Zusammenhang mit dem Inkrafttreten des revidierten Datenschutzgesetzes des Bundes stellte die SSO Fragen an die Datenschutzbeauftragte, beispielsweise zu ihrer Informationspflicht über gespeicherte Daten.

Die SSO vereint über 1000 Zahnärztinnen und Zahnärzte des Kantons. Im Rahmen des Notfalldiensts übermittelt sie die Personendaten der verfügbaren Zahnärztinnen und Zahnärzte an das Aerztefon, das diese direkt an die behandlungsbedürftigen Notfallpatientinnen und Notfallpatienten vermittelt.

Die SSO ist privatrechtlich organisiert. Für Private gelten grundsätzlich die Bestimmungen des Datenschutzgesetzes des Bundes (DSG). Die SSO wandte sich mit Fragen zum neuen DSG an die Datenschutzbeauftragte. Es war unklar, ob sie von jeder Zahnärztin und jedem Zahnarzt eine Einwilligung einholen muss, um ihre Daten an das Aerztefon weitergeben zu dürfen.

Wäre die Einwilligung jeder Zahnärztin oder jedes Zahnarztes notwendig, wäre ein Notfalldienst praktisch nicht durchführbar.

Die Abklärungen der Datenschutzbeauftragten ergaben, dass die betroffenen Zahnärztinnen und Zahnärzte für diese Datenbekanntgabe nicht einwilligen müssen. Die SSO wurde von der Gesundheitsdirektion mit der Organisation des zahnärztlichen Notfalldienstes beauftragt (§ 17 Abs. 1 lit. b und § 17a Abs. 1, GesG, LS 810.1 *(http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=810.1)*). Gestützt auf diesen Leistungsauftrag darf die SSO die Personendaten der Zahnärztinnen und Zahnärzte an das Aerztefon beziehungsweise an die Patientinnen und Patienten bekannt geben. Wäre die Einwilligung jeder Zahnärztin oder jedes Zahnarztes notwendig, die oder der sich für eine Notfallschicht zur Verfügung stellt, wäre ein Notfalldienst praktisch nicht durchführbar.

Variantenreiche Elektrizität

Elektrizitätsunternehmen sind teilweise öffentlich-rechtlich, andere sind privatrechtlich organisiert, etwa als Aktiengesellschaften oder Genossenschaften. Grundsätzlich unterstehen öffentlich-rechtliche Organisationen dem Gesetz über die Information und den Datenschutz (IDG). Privatrechtliche Organisationen unterstehen dem Datenschutzgesetz des Bundes (DSG).

Die Stromversorgung für private Haushalte untersteht nicht dem Wettbewerb. Sie können sich den Stromversorger nicht aussuchen. Unternehmen hingegen können das Elektrizitätsunternehmen frei wählen. Die Elektrizitätsunternehmen bearbeiten als Stromversorger also Personendaten sowohl im Monopol- als auch im Marktbereich. Zudem bearbeiten die Stromversorger weitere Personendaten, beispielsweise der Mitarbeitenden. Die Elektrizitätsunternehmen müssen deshalb für jeden Bereich evaluieren, welches Datenschutzrecht zur Anwendung gelangt und welche Aufsichtsbehörde zuständig ist.

Bearbeiten die öffentlich-rechtlich organisierten Elektrizitätsunternehmen Personendaten im Monopolbereich, tun sie dies im Rahmen des öffentlichen Leistungsauftrags. Hier unterstehen sie dem IDG. Bei den Aktivitäten im Marktbereich werden die Bestimmungen des DSG sinngemäss angewandt. Das IDG enthält diese Ausnahme für öffentliche Organe, die im Wettbewerb stehen. Für alle weiteren Bearbeitungen von Personendaten, etwa bei der Personaladministration, wird das IDG angewendet. Die Datenschutzbeauftragte des Kantons Zürich übt in allen Fällen die Aufsicht aus.

Bearbeiten privatrechtlich organisierte Elektrizitätsunternehmen Personendaten im Monopolbereich, unterstehen auch sie dem IDG. Bei ihren Aktivitäten im Marktbereich werden die Bestimmungen des DSG angewandt. Für alle weiteren Bearbeitungen von Personendaten, etwa bei der Personaladministration, wird ebenfalls das DSG angewandt. Die Datenschutzbeauftragte beaufsichtigt allerdings bei privatrechtlich organisierten Elektrizitätsunternehmen ausschliesslich die Aktivitäten im Monopolbereich. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beaufsichtigt alle weiteren Bearbeitungen von Personendaten.

Spezialfall Smart-Metering

Datenbearbeitungen im Zusammenhang mit Smart-Metering-Systemen werden durch das Bundesgesetz über die Stromversorgung dem DSG unterstellt (StromVG, SR 734.7 *(https://www.fedlex.admin.ch/eli/cc/2007/418/de)*). Dies ist eine weitere Variante, da hier auch Datenbearbeitungen im Monopolbereich nach den Vorgaben des Datenschutzgesetzes des Bundes beurteilt werden müssen.

Kunst, Video und Masterclass – Diversität bei der Sensibilisierung

Alljährlich am 28. Januar findet der Europäische Datenschutztag statt. Die Datenschutzbeauftragte nimmt dies zum Anlass, auf die Grundrechte auf Privatsphäre und informationelle Selbstbestimmung sowie ihre Bedeutung hinzuweisen. Im Jahr 2023 bot sich die spannende Möglichkeit, zusammen mit dem Verein We are AIA | Awareness in Art im Löwenbräuareal in Zürich die Data Privacy Art Days durchzuführen.

Kunst eröffnet einen neuen Blick auf Themen, die sonst bedrohlich und unnahbar erscheinen. Die Besucherinnen und Besucher konnten anhand der ausgestellten Kunstobjekte mit Expertinnen und Experten über die Macht von Daten, die Überwachung und die Manipulation durch Big-Tech-Firmen, die Nutzung und den Missbrauch von biometrischen Daten und die Chancen und Risiken von Algorithmen diskutieren. Mit dabei waren neben der Datenschutzbeauftragten auch Angela Müller von AlgorithmWatch, NZZ-Technologieredaktorin Ruth Fulterer, der WoZ-Journalist Florian Wüstholz, die Künstlerinnen Marta Revuelta und Lauren Huret, der Kurator des Hauses für elektronische Kunst in Basel Boris Magrini sowie die ETH-Professorin für Ethik, Technologie und Gesellschaft Margarita Boenig-Liptsin.

Karottensaft und Datenschutz

Im Datenschutz-Video-Wettbewerb entschied sich die Datenschutzbeauftragte dazu, einen Spezialpreis für Beiträge zu kreieren, die von Jugendlichen und im schulischen Umfeld produziert wurden. Dominika Blonski begründete den Entscheid: «Wir finden es toll, dass wir jedes Jahr grossartige, professionell produzierte Einsendungen bekommen. Daneben werden aber immer auch sehr gute Videos eingesandt, bei denen der Schnitt nicht immer ganz stimmt, der Ton Mängel hat oder die Geschichte hier und da etwas holpert, weil diese Videos durch Jugendliche produziert wurden, die wenig Erfahrung und Equipment haben. Diese Videos finden wir ebenso preiswürdig.» Der erste Spezialpreis ging an die Einsendung «Macht KI unser Leben einfacher?» von Maxime Kessler und Dorothea Röthlisberger. Die Jury bewertete den Einsatz der beschränkten Mittel als hohe Kunst. Hier kommen keine Schauspielerinnen zum Einsatz und das Video ist im hochformatigen Tiktok-Stil aufgenommen, aber es bringt die Botschaft auf den Punkt: Künstliche Intelligenz kann Menschen unterstützen. Doch was ist, wenn sie uns im Stich lässt? Ihr Video endet mit dem allseits bekannten «Hoppla, da ist was schiefgelaufen.»

Doch was ist, wenn die KI uns im Stich lässt? Das Video endet mit dem allseits bekannten «Hoppla, da ist was schiefgelaufen.»

Im stimmigen Rahmen des Kinos Riffraff überreichte Amila Redzic, SRF-Impact-Redaktorin und Social Media Host, die Preise an die Macherteams. Die Einsendung «Carrot Juice» wurde von der Fachjury am besten bewertet. Der Kurzfilm von Luis Oliveira, Amy Amstutz und Yann Belanga zeichne sich aus durch eine klare Botschaft sowie handwerkliche und schauspielerische Topleistungen. Der Jury gefielen die lustigen Dialoge und der Wortwitz. In ihrer Laudatio sagte Dominika Blonski: «Als Zuschauerin fiebert man mit, was der Grund sein könnte für die Werbung auf dem

Smartphone der Protagonistin. Der Beitrag fokussiert die Hauptmessage: Privacy matters.»

KI wird schon kontrolliert, allerdings nicht demokratisch

Schon seit Jahren sorgt die Datenschutzbeauftragten für die Präsenz der Anliegen des Datenschutzes in der Start-up-Szene. Am Digital Festival 2023 war Datenschutz eines der Schwerpunktthemen. Benjamin Walczak, Informatiker beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und Mitglied der KI-Taskforce des Bundesverbandes der deutschen Datenschutzbeauftragten, leitete eine Masterclass zum Thema Datenschutz by Design. Sein Rat: «Bei der Software-Entwicklung so früh wie möglich an den Datenschutz denken. Sonst wird`s später sehr schwierig.» Zudem diskutierte er im Panel «KI – Freund & Helfer» mit. Auf die Frage, ob und wie KI reguliert werden könne, meinte Benjamin Walczak: «KI-Systeme werden ja schon heute reguliert. Allerdings geschieht diese Regulierung durch Unternehmen. Was es nun braucht, ist eine demokratische Kontrolle.»

Sozialkreditsysteme in demokratischen Gesellschaften

In Zusammenarbeit mit der Paulus Akademie Zürich organisierte die Datenschutzbeauftragte die Podiumsdiskussion «Klima retten mit Belohnungssystemen». In den Städten Wien und Bologna wird auf freiwilliger Basis die Mobilität mit einer behördlichen App getrackt und umweltfreundliches Verhalten mit Gutscheinen belohnt. Inwieweit sind amtliche, digitale Sozialkreditsysteme mit unserer freien, demokratischen Gesellschaft vereinbar? Die Leiterin des Fachbereichs Wirtschafts- und Sozialethik der Paulus Akademie Dana Sindermann diskutierte mit der Datenschutzbeauftragten Dominika Blonski, dem Co-Präsidenten der Grünliberalen Partei Kanton Zürich Nicola Forster, dem Co-Präsidenten vom Verein für eine Schweiz ohne Sozialkreditsysteme Pascal Fouquet und dem ETH-Professoren für computerbasierte Soziologie Dirk Helbing. Die Effektivität solcher Sozialkreditsysteme zur Rettung des Planeten wurde bezweifelt. Daraus leitet sich ab, dass der tiefe Eingriff in die Privatsphäre durch das Tracking nicht verhältnismässig wäre.

Datenschutz und Sicherheit – wird jetzt alles gut?

Das Symposium on Privacy and Security fand 2023 zum 27. Mal statt. Der Fixstern für alle Fachpersonen öffentlicher Organe aus den Bereichen Datenschutz und Cybersicherheit konzentrierte sich auf zwei breit diskutierte, aktuelle Themen, die in der fortschreitenden Digitalisierung immer wichtiger werden.

Einerseits ging es um die Erwartungen an das neue Datenschutzgesetz des Bundes, das im September 2023 in Kraft trat. Andererseits wurden angesichts der immer häufiger bekannt gewordenen Hackerangriffe Fragen zur Cybersicherheit diskutiert.

Kantonsratspräsidentin Sylvie Matter begrüsste die rund 200 Teilnehmenden. Sie wies mit Blick auf die fortschreitende Digitalisierung darauf hin, dass immer mehr Daten gesammelt würden. «Je mehr Daten gesammelt werden, desto grösser wird das Risiko der Überwachung», warnte sie und fügte hinzu: «Dass riesige Datenmengen bei einigen wenigen Tech-Giganten liegen, muss uns Sorgen machen.»

Zu den Herausforderungen der digitalen Verwaltung gehört das Zusammenspiel von Recht und Technik. Hemmt der Datenschutz die Digitalisierung der Verwaltung, wie das oft vorgebracht wird? An der Front der Digitalisierung des Kantons Zürich sieht man das anders: «Das Datenschutzrecht unterstützt uns bei der Umsetzung der Digitalisierungsvorhaben sehr», erklärte Vanessa Rüegger, Leiterin Recht beim Team Digitale Verwaltung der Staatskanzlei. Sie fügte hinzu: «Nutzendenzentriert heisst für uns immer auch, grundrechtskonform zu arbeiten.»

«Das Datenschutzrecht unterstützt uns bei der Umsetzung der Digitalisierungsvorhaben sehr», erklärte Vanessa Rüegger, Leiterin Recht beim Team Digitale Verwaltung der Staatskanzlei.

Damit war die Datenschutzbeauftragte Dominika Blonski einverstanden: «Beim Datenschutzrecht geht es um die Konkretisierung der Grundrechte. Deshalb: Nur mit Datenschutz kann die Digitalisierung gelingen. Das Vertrauen der Bevölkerung steht auf dem Spiel.» Die Digitalisierungsstrategie des Zürcher Regierungsrats fasst die Leitsätze im Slogan «gemeinsam digital unterwegs» zusammen. Der Beauftragte von Bund und Kantonen für die Digitale Verwaltung Schweiz (DVS) Peppino Giarritta drückte es so aus: «Wenn der Mensch im Zentrum stehen soll bei Digitalisierungsvorhaben, dann braucht es auch die Bereitschaft zum Dialog mit den Menschen.» Zuerst müsse immer überlegt werden, wem denn die Digitalisierung nützen soll, meinte Catherine Pugin, Delegierte für Digitalisierung des Kanton Waadts. «Auch hier muss beim Staat der Mensch immer im Zentrum stehen.»

Das passende Schlusswort lieferte Isabel Wagner, Professorin für Cyber Security an der Universität Basel: «Ich wünschte mir, dass Software im Default-Zustand sicher ist und dass bei der Normalanwendung nichts schief gehen kann.»

Breites Aus- und Weiterbildungsportfolio

Die Datenschutzbeauftragte führte im Jahr 2023 insgesamt 27 Aus- und Weiterbildungen durch. Dazu gehört die 2. Zürcher Datenschutztagung mit Informationen zur praktischen Umsetzung von Informationssicherheit und Datenschutz. Die Tagung wird zusammen mit der ZHAW organisiert und richtet sich vor allem an Mitarbeitende der Gemeinden im Kanton Zürich. Neben einem Überblick über die aktuelle Bedrohungslage von Dr. Serge Droz, leitender technischer Berater beim Eidgenössischen Departement für auswärtige Angelegenheiten (EDA), gab es einen Einblick in die Verschlüsselungsmöglichkeiten durch Professor Rolf Oppliger vom Nationalen Zentrum für Cybersicherheit (NCSC).

In den Workshops bekamen die Teilnehmenden praktische Tipps für den Fall, dass sie gehackt wurden, aber auch dazu, wie Daten sicher gelöscht werden. Die Datenschutzbeauftragte präsentierte die Musterdokumente der Behörde, die Gemeinden bei der Umsetzung der Informationssicherheit unterstützen.

Weiterbildungsaktivitäten gab es zudem beim CAS MedLaw an der Universität Zürich, dem CAS Datenschutzverantwortliche, dem CAS Sozialhilfe und dem CAS KESR an der ZHAW. Für KV-Lernende im öffentlichen Bereich bot die Datenschutzbeauftragte das Modul Datenschutz und Amtsgeheimnis an. Ebenfalls an der KV Business School im Kurs zum Fachausweis öffentliche Verwaltung wurde ein Input zu Datenschutz und seinen Werkzeugen angeboten.

Genug Informationen für die Spitex

Ein Spital überwies eine Patientin an die Gemeinde-Spitex. Die Spitex war der Auffassung, dass das Spital nicht alle notwendigen Daten der Patientin zur Verfügung stellte. Sie könne die Person nicht richtig pflegen und ihrem Auftrag nicht nachkommen.

Eine Datenbekanntgabe zwischen den öffentlichen Organen muss sich auf eine rechtliche Grundlage stützen. In Einzelfällen kann allerdings auch im Rahmen der Amtshilfe um Informationen ersucht werden, wenn diese zur Erfüllung der gesetzlichen Aufgaben benötigt werden. Selbstverständlich muss vor jeder Datenbekanntgabe eine Interessensabwägung durchgeführt werden. Der Grundsatz der Verhältnismässigkeit verlangt, dass nur so viel Information weitergegeben wird wie nötig.

Vor jeder Datenbekanntgabe muss eine Interessenabwägung durchgeführt werden.

Der Informationsaustausch zwischen Spitälern und Spitex ist im Patientinnen- und Patientengesetz geregelt. Im vorliegenden Fall kam das Spital nach der Prüfung der Verhältnismässigkeit zum Schluss, dass nicht die gesamte Patientendokumentation für die Überweisung an die Spitex erforderlich ist.

Die Spitex hat die Möglichkeit, dem Spital inhaltliche Gründe vorzulegen, weshalb sie in welchen Fällen mehr Informationen benötigt, also eine weitergehende Datenbekanntgabe verhältnismässig wäre. Sie kann zudem in einzelnen Fällen zusätzliche Informationen im Rahmen der Amtshilfe anfordern.

Verhältnismässigkeit in Zeiten einer Epidemie

Der Bund arbeitet an der Teilrevision des Epidemiengesetzes. So soll die Schweiz besser auf eine zukünftige Epidemie reagieren können. Die Datenschutzbeauftragte nahm zuhanden der Gesundheitsdirektion Stellung zu den beabsichtigten Gesetzesänderungen.

Die Datenschutzbeauftragte begrüsst, dass der Bund für das Contact Tracing ein nationales Informationssystem bereitstellen wird und die Grundlagen entsprechend gesetzlich geregelt hat. Sie wies darauf hin, dass ein solches System besonders schützenswerte Personendaten wie die Gesundheitsdaten von erkrankten Personen bearbeiten wird. Deshalb sind beim Aufbau und beim Betrieb hohe Anforderungen zu erfüllen, was den Datenschutz durch technische und organisatorische Massnahmen anbelangt.

In der Vernehmlassungsvorlage wird explizit auf die Möglichkeit hingewiesen, im teilrevidierten Epidemiengesetz eine gesetzliche Grundlage für eine Contact-Tracing-App zu verankern. Das Bundesamt für Gesundheit sammelt derzeit die Rückmeldungen der Kantone, bevor es sich für oder gegen eine gesetzliche Grundlage zum digitalen Contract Tracing via Apps im Epidemiengesetz entscheidet. Die Datenschutzbeauftragte wies darauf hin, dass eine gesetzliche Grundlage für solche Apps notwendig ist. Diese kann jedoch kantonal oder auf Bundesebene geschaffen werden.

Auch Datenbearbeitungen mit Einwilligung müssen verhältnismässig sein

Der Revisionsentwurf des Epidemiengesetzes sieht bedeutende Änderungen beim Impfmonitoring vor. Heute müssen die Kantone bloss den Anteil der geimpften Personen erheben. In Zukunft sollen die kantonalen Behörden Daten über die Gesundheit einer geimpften Person erheben dürfen, wenn die betroffene Person dazu eingewilligt hat. Der Gesetzgeber will den Kantonen damit die Möglichkeit geben, eine grosse Menge an besonders schützenswerten Personendaten zu sammeln. Sie sollen dafür die Einwilligung der betroffenen Personen einholen.

Die Datenschutzbeauftragte beurteilt diese Regelung als bedenklich. Öffentliche Organe erfüllen gesetzliche Aufgaben. Sie dürfen Personendaten bearbeiten, wenn dies zur Erfüllung dieser Aufgaben notwendig ist. Besondere Personendaten dürfen nur bearbeitet werden, wenn dies in einem formellen Gesetz hinreichend bestimmt ist.

Wenn die vorgesehene Erweiterung der Datenbearbeitung beim Impfmonitoring geeignet und erforderlich zur Bekämpfung einer Epidemie ist, so ist sie verhältnismässig und bedarf keiner Einwilligung durch die betroffenen Personen. Wenn die Datenbearbeitung allerdings nicht verhältnismässig ist, dann darf sie nicht durchgeführt werden, auch wenn eine Einwilligung vorliegt.

Wenn die Erweiterung der Datenbearbeitung beim Impfmonitoring geeignet und erforderlich zur Bekämpfung einer Epidemie ist, so ist sie verhältnismässig und bedarf keiner Einwilligung.

Auskunftspflicht für infizierte und erkrankte Personen

Neu ist im Epidemiengesetz eine Auskunftspflicht für infizierte oder erkrankte Personen vorgesehen. Die betroffenen Personen werden verpflichtet, der kantonalen Behörde Auskunft über Kontakte zu anderen Personen zu geben. Diese Auskunftspflicht stellt einen tiefen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Die betroffenen Personen werden verpflichtet, Einblicke in die Zusammenstellung ihres Bekannten-, Freundes- und Familienkreises preiszugeben.

Die Datenschutzbeauftragte wies auf die Tragweite einer solche Pflicht hin. Sie sieht jedoch die Verhältnismässigkeit als gegeben, wenn alternative Massnahmen einschneidender wären. Dies wäre der Fall, wenn statt des Contact Tracings nur noch Kontaktverbote und Lockdowns möglich wären.