dsb
datenschutzbeauftragte
des kantons zürich

Tätigkeitsbericht 2022

Vorwort

Bild: Corinne Marrel, egovpartner

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 2022 bis und mit 31. Dezember 2022 ab.

Der 28. Tätigkeitsbericht erscheint in einem neuen Kleid und wird ausschliesslich online *(https://www.datenschutz.ch/tb/2022/neues-format-mit-neuen-moeglichkeiten)* unter www.datenschutz.ch publiziert.

Fragen zu Cloud-Diensten stehen mehr denn je im Vordergrund. Auch in sensitiven Bereichen wie Spitälern kommen vermehrt Cloud-Lösungen zum Einsatz. Damit die Grundrechte der Bürgerinnen und Bürger gewahrt bleiben, muss bei den juristischen und technischen Abklärungen methodisch sauber vorgegangen werden.

Die öffentlichen Organe sind in der Pflicht, die gesetzlichen Vorgaben einzuhalten und so die Freiheitsrechte der Bevölkerung zu garantieren.

Digitalisierungsvorhaben sind komplex. Sie vereinen viele Bestandteile, erleichtern Datenbearbeitungen und vernetzen Institutionen. Nicht immer ist transparent, was mit den Daten geschieht. Das Bedürfnis der öffentlichen Organe nach Beratung nimmt zu. Die Beratungen der Datenschutzbeauftragten werden umfangreicher.

Nicht nur für beabsichtigte Datenbearbeitungen sind gute Lösungen zu finden. Die Meldungen von Datenschutzvorfällen zeigen, dass auch bei den bestehenden Datenbearbeitungen grosser Nachholbedarf besteht.

Die öffentlichen Organe sind in der Pflicht, die gesetzlichen Vorgaben einzuhalten und so die Freiheitsrechte der Bevölkerung zu garantieren.

Dr. Dominika Blonski
Datenschutzbeauftragte des Kantons Zürich

Verantwortung übernehmen und die Zukunft gestalten

Lange vor Corona nahm die Digitalisierung in öffentlichen Institutionen Fahrt auf. Während der Pandemie wurde allen klar, welches Potenzial die neuen Technologien zur Lösung der aktuellen Herausforderungen mitbringen. So ist aus dem Streben nach einer digitalisierten Verwaltung ein Rennen geworden.

Druck von aussen spielt eine Rolle, geopolitische Fragen werden wichtig und übergeordnete Interessen grosser Konzerne bringen die öffentlichen Institutionen in Schwierigkeiten. Die Datenschutzbeauftragte berät und kontrolliert immer komplexere Projekte.

In diesem sehr dynamischen Umfeld ist es wichtig, dass sich die verantwortlichen Personen am gesetzlichen Regelwerk orientieren. Es bietet den besten Kompass. Damit wird auch das Vertrauen der Bevölkerung erhalten. Denn ohne Vertrauen der Bevölkerung wird die Arbeit von Politik und öffentlichen Institutionen schwierig.

> Es bezweckt,
>
> a. das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern sowie die Kontrolle des staatlichen Handelns zu erleichtern,
>
> b. die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Daten bearbeiten.
>
> § 1 Abs. 2 Gesetz über die Information und den Datenschutz (IDG)

Polizei: viele Möglichkeiten, besondere Risiken und ressourcensparendes Vorgehen

Der Polizei bieten die neuen Technologien viele interessante Möglichkeiten. Die Polizei bearbeitet meistens besonders schützenswerte Personendaten. Diese Digitalisierungsprojekte müssen der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden. Die Polizei will schnell vorwärts machen. Das ist verständlich. Die Vorhaben sind zum Teil sehr komplex, die Ressourcen der Datenschutzbeauftragten jedoch beschränkt. Die mit Umsicht erstellten Datenschutz-Folgenabschätzungen (DSFA) der Kantonspolizei *(https://www.datenschutz.ch/tb/2022/polizei-datenaustausch-ueber-kantonsgrenzen-und-staatsebenen-hinweg)* erleichtern nicht nur die Arbeit der Kantonspolizei, sondern auch jene der Datenschutzbeauftragten wesentlich.

Beim Polizei- und Justizzentrum (PJZ) treffen verschiedene öffentliche Institutionen mit besonderen Sicherheitsbedürfnissen aufeinander. Es beherbergt Abteilungen der Kantonspolizei, der Staatsanwaltschaft, des Justizvollzugs und des Zwangsmassnahmengerichts. Im PJZ arbeiten rund 2000 Personen. Neben den Mitarbeitenden müssen auch Besucherinnen und Besucher ins Gebäude hinein, dort an den richtigen Ort und dann wieder hinausgelangen.

Die im elektronischen Zugangssystem *(https://www.datenschutz.ch/tb/2022/pjz-besuchermanagement-einvernahmedisposition-und-sicherheitssupportsystem)* bearbeiteten Personendaten stehen oft in Zusammenhang mit einer Strafuntersu-

chung. Es werden sehr viele Daten bearbeitet und das System wird von verschiedenen Organisationen benutzt. Die Datenschutzbeauftragte verlangte eine klare Regelung der Aufbewahrungsfristen und der Löschung der Daten.

Datenschutz: Amtsstellen stehen in der Pflicht

Die Verantwortung für die Umsetzung der Hinweise der Datenschutzbeauftragten liegt bei den verantwortlichen öffentlichen Institutionen. Dies gilt auch beim Electronic Monitoring im Zivilrecht *(https://www.datenschutz.ch/tb/2022/electronic-monitoring-im-zivilrecht-oder-die-verantwortung-des-oeffentlichen-organs)*, das zur Überwachung des Rayonverbots eingesetzt wird. Das zuständige Amt für Justizvollzug und Wiedereingliederung (Juwe) legte das vorgesehene System der Datenschutzbeauftragten zur Vorabkontrolle vor. Im Jahr 2018 beriet die Datenschutzbeauftragte das Juwe zum Electronic Monitoring im Zivilrecht. Sie wies damals darauf hin, dass das System mehr Daten bearbeitet, als für die Überwachung des Rayonverbots nötig sind. Beispielsweise werden auch die Standortdaten ausserhalb des verbotenen Gebiets aufgezeichnet. Dies ist rechtswidrig. Zudem wird Kartenmaterial von Google Maps verwendet. Es wird nicht nachgewiesen, dass die Daten der überwachten Personen nicht an den privaten Anbieter weitergeleitet werden. Die Datenschutzbeauftragte hatte diesen Zustand 2018 bemängelt. In der Vorabkontrolle im Jahr 2022 stellte sie fest, dass die Mängel nicht behoben worden sind.

Cloud-Lösungen: Gesetze respektieren, Geheimnispflichten einhalten

Bis vor wenigen Jahren wurden Cloud-Produkte punktuell eingesetzt. Jetzt nehmen gesamtheitliche Lösungen überhand. Microsoft 365 ist dafür nur eines der Beispiele, wenn auch das dominanteste. Lösungen, die darauf ausgelegt sind, alle Datenbearbeitungen zu integrieren, bringen auch höhere Risiken mit sich. Die enge Verzahnung der Dienste untereinander erhöht die Gefahr, dass Dokumente durchrutschen, die vertraulich oder durch eine besondere Geheimnispflicht geschützt sind.

Bei der Abklärung der Frage, ob eine Datenbearbeitung in die Cloud *(https://www.datenschutz.ch/tb/2022/risiken-und-regeln)* ausgelagert werden kann, ist ein methodisches Vorgehen zu wählen. Zuerst muss eine Analyse der Rechtsgrundlagen durchgeführt werden. Dafür müssen die geltenden Geheimnispflichten eruiert werden. Zugriffsmöglichkeiten von ausländischen Behörden (CLOUD Act) sind festzustellen. Erst danach kann und muss über Risikominderung durch technische und organisatorische Massnahmen nachgedacht werden.

Bei Personendaten, die unter einem besonderen Amtsgeheimnis oder einem Berufsgeheimnis stehen, hält das Gesetz fest: Die verantwortliche Person macht sich strafbar, wenn sie Unberechtigten auch nur die Möglichkeit gibt, solche Daten zur Kenntnis zu nehmen. So ist die Entscheidung einfach. Daten unter einem besonderen Amtsgeheimnis oder einem Berufsgeheimnis können nur ausgelagert werden, wenn sie verschlüsselt sind und ausschliesslich die verantwortliche Person oder ihre Hilfspersonen den Schlüssel kennen.

Die gängigsten gesamtheitlichen Cloud-Lösungen stammen von US-amerikanischen Unternehmen. Sie unterstehen dem CLOUD Act. Der CLOUD Act ermöglicht amerikanischen Behörden, Zugriff auf die Daten zu verlangen, unabhängig davon, wo sie gespeichert sind. Damit werden die Abkommen zur Rechtshilfe umgangen. Das Vorgehen verstösst gegen die schweizerische Rechtsordnung. Vertragliche Absicherungen helfen nicht. Es steht dem US-amerikanischen Unternehmen nicht frei, wegen eines Vertrags das Gesetz der USA nicht einzuhalten.

Die Rechtsfrage kann nicht mit Wahrscheinlichkeitsrechnungen umgangen werden. Wenn ein Zugriff rechtswidrig ist, hilft es nicht, dass die Wahrscheinlichkeit eines solchen Zugriffs klein sein könnte. Ein öffentliches Organ hat sich immer rechtmäs-

sig zu verhalten (Legalitätsprinzip). Die Aussagen zur Wahrscheinlichkeitsberechnung im Regierungsratsbeschluss zu Microsoft 365 (RRB 542/2022) wurden inzwischen relativiert. Die Finanzdirektion schränkte mit der Allgemeinen Nutzungsrichtlinie Microsoft 365 vom 29. Juni 2022 die Nutzung der Dienste ein. Dies entspricht auch der Regelung, die für die Bundesverwaltung gilt.

Keine Übersicht über die Verwendung von Microsoft 365

Ist eine neue Bearbeitung von Personendaten beabsichtigt, dann muss das öffentliche Organ eine Datenschutz-Folgenabschätzung (DSFA) durchführen. Eine sorgfältig durchgeführte DSFA zur Einführung von Microsoft 365 würde in den meisten Fällen auf erhöhte Risiken hinweisen. Dies, weil einerseits eine grosse Menge an Personendaten bearbeitet wird. Oft kommt dazu, dass es sich um besonders schützenswerte Personendaten und solche unter besonderen Geheimnispflichten handelt. Andererseits werden neue Technologien mit neuen Möglichkeiten eingesetzt. In diesen Fällen ist das Projekt der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Bisher reichte jedoch kein öffentliches Organ im Kanton Zürich der Datenschutzbeauftragten ein Projekt zur Einführung von Microsoft 365 *(https://www.datenschutz.ch/tb/2022/risiken-und-regeln)* zur Vorabkontrolle ein.

Intransparenz von Anbietern

Die Beurteilung von Cloud-Projekten ist aufwendig. Die integrierten Cloud-Lösungen zeichnen sich durch eng verzahnte und beinahe unüberblickbare Verbindungsuniversen aus. Die einfachen und fast uneingeschränkten Möglichkeiten zum Datenaustausch bergen eine Vielzahl an Risiken für widerrechtliche Datenbekanntgaben. Die Anbieter sind zudem nicht bereit, transparent zu kommunizieren, wofür sie etwa die Randdaten über die Nutzung der Dienste *(https://www.datenschutz.ch/tb/2022/besonderen-schutz-fuer-religioese-aktivitaeten)* genau verwenden. Die öffentlichen Organe tragen jedoch die Verantwortung für ihre Daten, auch wenn sie diese in der Cloud bearbeiten. So besteht eine Kluft zwischen dem Auftrag des Organs und den realen Möglichkeiten.

Entscheiden, wie wir in Zukunft leben wollen

Als Grund für Digitalisierungsprojekte wird angeführt, dass Private es auch so machen. Ein weiteres Argument ist, dass die Attraktivität der öffentlichen Organe als Arbeitgeberinnen oder als Arbeitgeber sonst gefährdet sei. Solche Begründungen werden der Tragweite der Entscheidungen nicht gerecht. Es geht immerhin darum, wie wir mit den Personendaten der Menschen im Kanton Zürich umgehen. Sie müssen den öffentlichen Organen viele und oft sehr persönliche Informationen anvertrauen.

Wir stehen mitten in einem spannenden und herausfordernden Prozess des Strukturwandels. Wie wir welche Technologie zu welchem Zweck einsetzen, bestimmt, wie wir in Zukunft zusammenleben werden. Deshalb lohnt sich, zu diskutieren *(https://www.datenschutz.ch/tb/2022/mehr-lebensqualitaet)*, welche Werte wir schützen und fördern wollen. Dann können wir entscheiden.

Umfangreiche Beratungen und Vorabkontrollen

Die im Kontinuierlichen Entwicklungs- und Finanzplan (KEF) für das Jahr 2022 festgelegten Indikatoren der Datenschutzbeauftragten zeigen eine stabile Entwicklung.

Beratungen und Vorabkontrollen

Wenn öffentliche Organe neue Datenbearbeitungen vorsehen, sind sie verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen. Damit werden die Risiken des Projekts für die Privatsphäre eingeschätzt und Massnahmen definiert, um die Risiken zu minimieren. Wenn mit der DSFA besondere Risiken festgestellt werden, ist das Projekt der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten.

Die Digitalisierungsvorhaben werden zunehmend komplexer. Die Datenschutzbeauftragte begleitet die neuen Vorhaben immer häufiger mit aufwendigen Beratungen. Andererseits bearbeitet sie mehr und weitreichendere Vorabkontrollen.

Anzahl Beratungen

KEF	2021	2022
750	753	569

Kontrollen

Die Kontrolltätigkeit konnte im Berichtsjahr stabil ausgebaut werden. Die pandemie-bedingten Einschränkungen sind weggefallen. Da Kontrollen über einen längeren Zeitraum verlaufen und im KEF nur die abgeschlossenen Kontrollen registriert sind, wird sich die zunehmende Kontrolltätigkeit erst in den nächsten Jahren deutlich abzeichnen.

Anzahl Kontrollen

KEF	2021	2022
60	22	24

Aus- und Weiterbildungen

Die Aus- und Weiterbildungen konnten auch im letzten Jahr auf hohem Niveau weitergeführt werden. Die Datenschutzbeauftragte stärkt mit ihrem Weiterbildungs- und Informationsengagement die Datenschutzkompetenz bei den Mitarbeitenden der öffentlichen Organe. Sie werden befähigt, ihre Verantwortung in der Digitalisierung wahrzunehmen und die Anforderungen des Datenschutzes und der Informationssicherheit in ihrem Alltag zu meistern.

Anzahl Aus- und Weiterbildungen

KEF	2021	2022
20	29	29

Website-Besuche

Die Datenschutzbeauftragte sieht eine positive Entwicklung bei der Sensibilisierung der Mitarbeitenden von öffentlichen Organen, aber auch der Bevölkerung. Die steigende Anzahl Zugriffe auf die Website www.datenschutz.ch zeigt, dass der Informationsbedarf bei Mitarbeitenden von öffentlichen Organen und der Bevölkerung konstant hoch bleibt.

Anzahl Website-Besuche

KEF	2021	2022
45000	39225	49585

Das neue IDG nimmt Gestalt an

Das Gesetz über die Information und den Datenschutz wird totalrevidiert. In der Vernehmlassung wurden zahlreiche Vorschläge eingebracht, welche die unterschiedlichen Herausforderungen von Öffentlichkeitsprinzip und Datenschutz im Alltag offenbaren.

Im Jahr 2020 initiierte der Regierungsrat die Totalrevision des Gesetzes über die Information und den Datenschutz (IDG). Das Gesetz soll an die Bedürfnisse der modernen Verwaltung angepasst werden. Die Datenschutzbeauftragte war in der Arbeitsgruppe zur Erarbeitung des Entwurfs zum neuen IDG sowie im Steuerungsausschuss vertreten. Im Sommer 2022 wurde die Vernehmlassung zum Entwurf durchgeführt.

Die zahlreichen Eingaben in der Vernehmlassung zeigen, dass das Öffentlichkeitsprinzip und der Datenschutz breite Kreise interessieren und beschäftigen. Die Totalrevision des IDG wird als Chance wahrgenommen, Vorschläge und Anliegen zur Verbesserung einzubringen.

Die Datenschutzbeauftragte platzierte einige grundlegende Fragen in der Arbeitsgruppe und im Steuerungsausschuss. Nicht alle wurden berücksichtigt. Sie hat diese in ihrer Stellungnahme zum Vernehmlassungsentwurf noch einmal aufgegriffen.

Die Datenschutzbeauftragte begrüsste die Stärkung des Öffentlichkeitsprinzips, indem eine unabhängige Aufsicht geschaffen wird. Damit erhalten neben der kantonalen Verwaltung auch die Gemeinden sowie die Bürgerinnen und Bürger eine Anlaufstelle für den Datenschutz und das Öffentlichkeitsprinzip, was die Wahrnehmung ihrer Rechte erleichtert. Weiter begrüsste die Datenschutzbeauftragte die Regulierung des Zugangs zu offenen Behördendaten und die Möglichkeit, besondere Personendaten im Rahmen von Pilotversuchen zu bearbeiten.

Damit erhalten neben der kantonalen Verwaltung auch die Gemeinden sowie die Bürgerinnen und Bürger eine Anlaufstelle für den Datenschutz und das Öffentlichkeitsprinzip, was die Wahrnehmung ihrer Rechte erleichtert.

Sie bedauerte, dass das bestehende Normkonzept des IDG aufgehoben wurde und die Bereiche Öffentlichkeitsprinzip und Datenschutz getrennt und in separaten Abschnitten geregelt wurden. Der Zugang zu Personendaten und Informationen und der Schutz der Informationen betrifft aus der Sicht der Bürgerinnen und Bürger sowie der Verwaltung die gleichen Prozesse. Das Gesetz wird damit gegenüber heute unübersichtlicher und die Anwendung wird erschwert. Auch die Weiterentwicklung der Gesetzgebung wird erschwert, da neue Phänomene, wie sich dies bereits beim Zugang zu offenen Behördendaten zeigt, weder dem einen noch dem anderen Kapitel des Gesetzes treffend zugeordnet werden können. Auch weitere regulatorische Anforderungen beispielsweise bei der Anwendung von Künstlicher Intelligenz werden schwieriger in das Gesetz einzupassen sein.

Die Bereiche Öffentlichkeitsprinzip und Datenschutz werden voneinander getrennt. Dadurch werden weitere regulatorische Anforderungen beispielsweise bei der Anwendung von Künstlicher Intelligenz schwieriger in das Gesetz einzupassen sein.

In ihrer Stellungnahme wies die Datenschutzbeauftragte darauf hin, dass eine Datenbekanntgabe im Rahmen der Amtshilfe ausschliesslich im Einzelfall zulässig ist. Im vorliegenden Gesetzesentwurf ist die Einschränkung auf den Einzelfall nicht mehr enthalten. Eine systematische Bekanntgabe von Personendaten gestützt auf die Amtshilfe widerspricht dem Sinn und Zweck des Amtsgeheimnisses. Die Amtshilfe stellt einen Auffangtatbestand dar. Sie kommt dann zum Einsatz, wenn keine gesetzliche Grundlage für eine Datenbekanntgabe vorliegt, im Einzelfall aber ein überwiegendes öffentliches Interesse an einer Bekanntgabe besteht. Wenn die Daten systematisch ausgetauscht werden sollen, ist dafür eine Rechtsgrundlage zu schaffen.

Ein anderer Einwand der Datenschutzbeauftragten war bereits berücksichtigt worden. Er betraf die Einwilligung als Grundlage für die Bearbeitung von Personendaten. Die Datenbearbeitung gestützt auf die Einwilligung der betroffenen Person ist nicht mit dem verfassungsrechtlichen Legalitätsprinzip vereinbar. Öffentliche Organe benötigen für ihr Handeln eine Rechtsgrundlage.

Die Datenschutzbeauftragte wird die weitere Entwicklung des Entwurfs weiter beobachten und begleiten. Sie wird ihr Fachwissen und die Sicht der Aufsichtsbehörde auch im politischen Prozess einbringen.

Unabhängig von der laufenden Totalrevision des IDG trat im Jahr 2022 eine Änderung der Kostenregelung für den Informationszugang und den Zugang zu den eigenen Personendaten in Kraft. Für Gesuche von Privatpersonen werden in der Regel keine Kosten mehr erhoben. Der gesuchstellenden Person kann eine angemessene Gebühr auferlegt werden, wenn die Bearbeitung eines Gesuches einen erheblichen Aufwand verursacht und in keinem vertretbaren öffentlichen Interesse steht. Die Datenschutzbeauftragte begrüsste diese Regelung. Die Kostenlosigkeit auch für Informationszugangsgesuche ist im Sinne der Bürgerinnen und Bürger. Sie stärkt das verfassungsmässige Recht auf Informationszugang.

Weitere Informationen der Datenschutzbeauftragten zur Revision des Gesetzes über die Information und den Datenschutz:

- Für ein zukunftsgerichtetes neues IDG, in: Tätigkeitsbericht 2021, Seite 8
- Stellungnahme Totalrevision Gesetz über die Information und den Datenschutz

Das Video auf dieser Seite ist auf der datenschutzkonformen, schweizerischen Videoplattform Switchtube veröffentlicht, weshalb keine Zwei-Klick-Lösung eingesetzt werden muss.

Polizei: Datenaustausch über Kantonsgrenzen und Staatsebenen hinweg

Die Polizei muss immer mehr interkantonal agieren können. Auch der Austausch von besonderen Personendaten findet über die Kantonsgrenzen hinweg statt. Die heutigen technischen Möglichkeiten erleichtern diesen Austausch. Allerdings müssen die rechtlichen Rahmenbedingungen beachtet werden.

Für den Datenaustausch mit Behörden anderer Kantone und des Bundes über die geplanten Plattformen und durch die Verknüpfung polizeilicher Systeme müssen zuerst die erforderlichen Rechtsgrundlagen geschaffen werden. Zudem sind Fragen der Verfassungsmässigkeit zu klären.

Bei kantonsübergreifend geplanten Projekten der Kantonspolizei arbeitete die Datenschutzbeauftragte mit den Datenschutzbehörden der anderen Kantone zusammen. Sie brachte ihre Sicht im Rahmen einzelner Geschäfte ein, aber auch über die Konferenz der schweizerischen Datenschutzbeauftragten privatim.

Die Datenschutzbeauftragte ist involviert in ein Projekt der Kantonspolizei zur Beschaffung einer neuen Lagebildsoftware durch Polizeikorps und Blaulichtorganisationen verschiedener Kantone und Städte. Sie koordinierte die Stellungnahmen der beteiligten Datenschutzbehörden zuhanden der Projektleitung.

Die detaillierten und mit Umsicht erstellten Datenschutz-Folgenabschätzungen der Kantonspolizei erleichterten nicht nur die Arbeit der Kantonspolizei, sondern auch jene der Datenschutzbeauftragten wesentlich.

Eine seriöse Datenschutz-Folgenabschätzung erleichtert die Arbeit

Die Kantonspolizei legte der Datenschutzbeauftragten im Jahr 2022 zahlreiche Vorhaben zur Prüfung vor. Die Komplexität der Vorhaben beanspruchte die Ressourcen der Datenschutzbeauftragten stark. Sie führte unter anderem eine Vorabkontrolle eines Systems für die automatisierte Personensicherheitsprüfung durch und prüfte ein neues System zur Fotografie bei der erkennungsdienstlichen Behandlung sowie eine Applikation zur taktischen Kriminalanalyse. Sie stellte fest, dass die Vorhaben der Kantonspolizei die Vorgaben des Datenschutzes wie auch der Informationssicherheit in hohem Mass erfüllen. Die detaillierten und mit Umsicht erstellten Datenschutz-Folgenabschätzungen der Kantonspolizei erleichterten nicht nur die Arbeit der Kantonspolizei, sondern auch jene der Datenschutzbeauftragten wesentlich. Dadurch konnte sie die grosse Anzahl an Vorhaben speditiv bearbeiten. Die Kantonspolizei konnte diese ebenso speditiv umsetzen.

Anpassung der Rechtslage durch die Revision des Polizeigesetzes

Die Datenschutzbeauftragte begleitete die Sicherheitsdirektion und die Kantonspolizei bei der Revision des Polizeigesetzes. Die Revision steht ebenfalls in Zusammenhang mit den Bestrebungen zum interkantonalen polizeilichen Informationsaustausch. Mit der Revision sollen unter anderem Grundlagen geschaffen werden, die der Polizei im Rahmen der Amtshilfe einen Datenaustausch mit anderen Polizeien sowie Behörden von Bund und Kantonen im Abrufverfahren erleichtern sollen. Ihre Datenbanken sollen verknüpft werden können. Weiter sollen die Fahrzeugfahndung

und die Verkehrsüberwachung (AFV) automatisiert werden. Die Videoaufnahmen aus der Verkehrsleitung sollen neu für weitere Zwecke genutzt werden können.

Die Datenschutzbeauftragte wurde von der Sicherheitsdirektion im Jahr 2021 zur Stellungnahme eingeladen. Sie hielt fest, dass der Vorentwurf zu diesem Zeitpunkt die Anforderungen an die Rechtsgrundlagen in einigen Punkten nicht erfüllte. In einer zweiten Stellungnahme zu einem angepassten Vorentwurf waren einzelne Bestimmungen verbessert worden. Im direkten Austausch unterstützte die Datenschutzbeauftragte die Kantonspolizei bei der Redaktion einzelner Bestimmungen. Zum Datenaustausch verwies sie auf die kantonsübergreifenden Projekte.

Das Video auf dieser Seite ist auf der datenschutzkonformen, schweizerischen Videoplattform Switchtube veröffentlicht, weshalb keine Zwei-Klick-Lösung eingesetzt werden muss.

PJZ: Besuchermanagement und Sicherheitssupportsystem

Die Polizei und die Institutionen des Amtes für Justizvollzug und Wiedereingliederung (Juwe) bearbeiten grosse Mengen an besonders sensitiven Personendaten von einer grossen Anzahl Personen. Die Technologie ermöglicht, immer mehr Daten, immer ausgiebiger zu bearbeiten und einfacher auszutauschen. Dies zeigt sich auch in den Beratungsanfragen und Vorabkontrollen in Zusammenhang mit den Polizei- und Justizzentrum (PJZ).

Die Einhaltung der datenschutzrechtlichen Bestimmungen stellt nicht nur die Polizei und die Justizvollzugsbehörden vor immer grössere Aufgaben. Die Anzahl und die Komplexität der Projekte fordern auch die Ressourcen der Datenschutzbeauftragten.

Besuchermanagement und Einvernahmedisposition

Das neu erstellte Polizei- und Justizzentrum Zürich (PJZ) beherbergt verschiedene Abteilungen der Kantonspolizei, der Staatsanwaltschaft, des Justizvollzugs und Teile des Zwangsmassnahmengerichts. Im PJZ arbeiten rund 2000 Personen. Neben den Mitarbeitenden, die täglich ein- und ausgehen, müssen auch Besucherinnen und Besucher ins Gebäude hinein, dort an den richtigen Ort und dann wieder hinausgelangen.

Die Sicherheitsanforderungen des Gebäudes stellen hohe Anforderungen an das System, in dem die Einvernahmedisposition und das Besuchermanagement bearbeitet werden. Ebenso hohe Anforderungen stellen die datenschutzrechtlichen Vorgaben. Die in diesem System bearbeiteten Personendaten stehen zu einem grossen Teil im Zusammenhang mit einer Strafuntersuchung. Sie stellen besondere Personendaten dar. Ausserdem wird eine sehr grosse Anzahl Personendaten bearbeitet und das System wird von drei Organisationen genutzt, nämlich der Kantonspolizei, der Staatsanwaltschaft und dem Gefängnis Zürich West. Die Nutzung des Systems birgt besondere Risiken für die Grundrechte der betroffenen Personen. Die Datenschutzbeauftragte führte deshalb eine Vorabkontrolle durch (§ 10 Abs. 2 IDG).

Die in diesem System bearbeiteten Personendaten stehen zu einem grossen Teil im Zusammenhang mit einer Strafuntersuchung. Sie stellen besondere Personendaten dar.

Die Datenschutzbeauftragte stellte fest, dass das System den rechtlichen sowie organisatorischen und technischen Anforderungen grundsätzlich genügte. Sie wies darauf hin, dass die rechtlichen Grundlagen für die Datenbearbeitung in den Unterlagen nicht aufgeführt waren. Weiter machte sie darauf aufmerksam, dass die Aufbewahrungsfrist und die Löschung der Personendaten nicht geregelt waren. Weitere Hinweise betrafen einzelne Punkte organisatorischer und technischer Natur.

Eine Privatperson wandte sich nach Inbetriebnahme des Systems an die Datenschutzbeauftragte mit der Frage, ob mit ihr abgesprochen sei, dass die Informationen über die personalisierten Zu- und Austritte im System des PJZ fünf Jahre aufbewahrt bleiben. Die Datenschutzbeauftragte informierte die Person, dass sie in ihrem Bericht auf die fehlende Regelung in diesem Punkt hingewiesen habe. Die Um-

setzung ihrer Hinweise liege in der Verantwortung des öffentlichen Organs. Sie verwies die anfragende Person an die zuständige Stelle.

Pünktlich am richtigen Ort – das Sicherheitssupportsystem Gefängnis Zürich West

Im PJZ befindet sich auch das Gefängnis Zürich West. Es enthält auf sechs Stockwerken Zellen für die Unterbringung vorläufig festgenommener Personen sowie für Personen in Untersuchungshaft. Der Betrieb erfordert eine minutiöse Planung der Zellenbelegung sowie der Personenbewegungen. Dazu gehören Einvernahmen, Gespräche mit Rechtsvertreterinnen und Rechtsvertretern und medizinische Untersuchungen. Für die reibungslose Organisation des Betriebs wurde ein System beschafft, in dem die Betreuungspersonen die Termine der inhaftierten Personen planen. Sie können jederzeit feststellen, welche Person sich wann wo befindet. Das System offenbart den Betreuenden eine grosse Menge besonderer Personendaten über die inhaftierten Personen.

Die Datenschutzbeauftragte wurde vom Amt für Justizvollzug und Wiedereingliederung (Juwe) in einem frühen Projektstadium einbezogen. Sie konnte so über wichtige datenschutzrechtliche Grundsätze und Vorgaben informieren. Im späteren Verlauf des Projektes nahm sie eine Vorabkontrolle vor. Sie wies darauf hin, dass die Rechtsgrundlagen für die Verwendung von biometrischen Daten wie Fingerabdrücken und Iris-Scans zur Identifizierung der inhaftierten Personen fehlten. Ein so schwerer Eingriff in die Grundrechte muss in einem formellen Gesetz geregelt, im öffentlichen Interesse und verhältnismässig sein (Art. 36 Bundesverfassung). Die in den Dokumenten dargelegten Rechtsgrundlagen erfüllten diese Anforderungen nicht. Das Juwe erklärte später, dass die Bearbeitung biometrischer Daten zur Identifizierung nicht vorgesehen sei.

Die Datenschutzbeauftragte erachtete als unverhältnismässig, dass im System die vorgesehene grosse Anzahl von Datenkategorien über die inhaftierten Personen bearbeitet wird. Ihr wurde nicht genügend dargelegt, dass diese Daten geeignet und erforderlich sind, um den Zweck zu erreichen. Sie beurteilte den Einsatz von Mitarbeitenden zweier externer Firmen als kritisch, da diese Personen Zugriff auf das System und damit auf die enorme Menge besonders sensitiver Personendaten haben. Schliesslich war die Löschung der Personendaten aus dem System nach Abschluss eines Geschäftsfalles ungenügend geregelt.

Electronic Monitoring im Zivilrecht oder die Verantwortung des öffentlichen Organs

Eine Ergänzung des Zivilgesetzbuches (ZGB) erlaubt Electronic Monitoring auch im Zivilrecht, etwa zur Überwachung eines Rayonverbots. Das Amt für Justizvollzug und Wiedereingliederung (Juwe) ist die Vollzugsbehörde des Electronic Monitorings. Es legte das Projekt der Datenschutzbeauftragten zur Vorabkontrolle vor.

Ein interdisziplinäres Team der Datenschutzbeauftragten aus den Bereichen Recht und Informationssicherheit überprüft die anspruchsvollen Vorhaben des Juwe. In ihren Berichten und Stellungnahmen ging die Datenschutzbeauftragte auf datenschutzrechtliche Grundlagen ein. Die Umsetzung der Hinweise der Datenschutzbeauftragten in ihren Stellungnahmen und Berichten liegt in der Verantwortung der öffentlichen Organe. Bei Fragen zur Umsetzung steht die Datenschutzbeauftragte zur Verfügung.

Die Datenschutzbeauftragte beriet das Juwe im Jahr 2018 zum Electronic Monitoring im Zivilrecht. Sie stellte fest, dass das System mehr Überwachungsdaten erfasst, als zur Aufgabenerfüllung notwendig sind. Die überschüssige Datenbearbeitung ist unverhältnismässig und daher rechtswidrig. Zudem sei nicht sichergestellt, dass die überschüssigen Überwachungsdaten nicht an andere Behörden weitergegeben werden.

Im Bericht zur Vorabkontrolle wies die Datenschutzbeauftragte im Jahr 2022 erneut darauf hin, dass dies verhindert werden muss und die sofortige Löschung der widerrechtlich erhobenen Personendaten sicherzustellen ist. Sie stellte zudem fest, dass trotz ihres Hinweises im Jahr 2018 immer noch das Kartenmaterial von Google Maps benutzt wurde, ohne dass nachgewiesen wurde, dass keine Standortdaten an Google gesendet werden. Die Informationen aus dem Electronic Monitoring sind in jedem Fall besonders schützenswerte Personendaten. Eine Weiterleitung der Daten an Google stellt eine Verletzung der Grundrechte der betroffenen Personen dar.

Die Informationen aus dem Electronic Monitoring sind in jedem Fall besonders schützenswerte Personendaten.

Weiter stellte die Datenschutzbeauftragte Mängel bei der Datenaufbewahrung und der Einhaltung der Löschungsfrist fest. Die Daten werden auf unbestimmte Zeit aufbewahrt und auch für andere Zwecke verwendet. Dies verstösst gegen den Zweckbindungsgrundsatz des Gesetzes über die Information und den Datenschutz (IDG). Es verstösst aber auch gegen die Bestimmungen zur elektronischen Überwachung im Zivilgesetzbuch. Die aufgezeichneten Daten dürfen nur zur Durchsetzung des Verbots verwendet werden und müssen spätestens zwölf Monate nach Abschluss der Massnahme gelöscht werden (Art. 28c Abs. 3 ZGB).

Die Datenschutzbeauftragte musste die unterschiedlichen Rechtsansprüche grundlegend erläutern, die sich ergeben aus dem Recht auf informationelle Selbstbestimmung (Art. 13 Bundesverfassung) und aus dem Öffentlichkeitsprinzip (Art. 49 Kantonsverfassung). Es besteht das Risiko, dass aufgrund des fehlenden Verständnisses der zuständigen Behörden die individuellen Rechte betroffener Personen nicht beachtet werden. Die Datenschutzbeauftragte wird die Erkenntnisse aus diesen Beratungen in ihrer Geschäfts- und Kontrollplanung berücksichtigen.

Risiken und Regeln

Die Cloud ist im Verwaltungsalltag angekommen. Viele Anwendungen laufen bereits in der Cloud, weitere werden getestet und manches ist in Planung. Doch Fragen zu den Möglichkeiten und Risiken der Auslagerung in die Cloud gibt es viele. Kein anderes Thema beschäftigte die Datenschutzbeauftragte 2022 häufiger.

Das Thema Cloud betrifft alle öffentlichen Organe. Viele wollten im Jahr 2022 ihre Unsicherheiten zum Einsatz der Cloud mit der Datenschutzbeauftragten besprechen: Gemeinden, Spitäler, Schulen und Hochschulen, Kirchen, Kindes- und Erwachsenenschutzbehörden sowie Altersheime und Institutionen, die im Leistungsauftrag für öffentliche Organe tätig sind. Oft betrafen die Anfragen Microsoft 365, aber auch zu anderen Anwendungen gab es Fragen.

Unabhängig von der Anwendung drehten sich die Fragen vor allem um zwei Punkte: Welche Daten dürfen in die Cloud? Was muss bei der Auslagerung in die Cloud beachtet werden? Die Antworten sind vom Kontext abhängig. Die Überlegungen sind aber immer gleich.

Bei der Auslagerung sind zwei Anforderungen zu beachten: Erstens dürfen der Auslagerung keine rechtlichen Bestimmungen entgegenstehen. Dazu gehören beispielsweise Geheimnispflichten. Zweitens bleibt das öffentliche Organ nach der Auslagerung für die Personendaten verantwortlich und muss die Einhaltung des Datenschutzes sicherstellen.

Erstens dürfen der Auslagerung keine rechtlichen Bestimmungen entgegenstehen. Zweitens bleibt das öffentliche Organ nach der Auslagerung für die Personendaten verantwortlich.

Bei der Abklärung der Frage, ob und welche Daten in der Cloud bearbeitet werden können, ist methodisch vorzugehen. In der Rechtsgrundlagenanalyse ist zu beurteilen, wie weit Geheimhaltungspflichten oder Zugriffsmöglichkeiten von ausländischen Behörden einer Auslagerung entgegenstehen. Erst wenn die Rechtsgrundlagenanalyse ergibt, dass Daten in der Cloud bearbeitet werden dürfen, folgt die Schutzbedarfsanalyse, auch Risikoanalyse genannt. Damit wird festgelegt, mit welchen organisatorischen und technischen Massnahmen die Risiken zu minimieren sind. In einem Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) werden die Resultate der Schutzbedarfsanalyse zusammengefasst. Das ISDS-Konzept ist die Grundlage für die Umsetzung des Projekts. Für die beabsichtigte Datenbearbeitung muss nun eine Datenschutz-Folgenabschätzung (DSFA) erstellt werden (§ 10 Abs. 1 IDG). Wenn besondere Risiken für die Grundrechte der betroffenen Personen bestehen, sind das ISDS-Konzept und die DSFA der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Geheimnispflichten einhalten

Geheimnispflichten können der Auslagerung entgegenstehen. Dazu gehören das Amtsgeheimnis, die besonderen Amtsgeheimnisse wie das Steuergeheimnis oder das Sozialhilfegeheimnis sowie das Berufsgeheimnis, das besonders bei Spitälern, schulärztlichen Diensten, psychologischen Beratungsstellen oder ähnlichen Institutionen zu beachten ist. Wenn bei der Auslagerung eine technische Lösung einge-

setzt wird, die verhindert, dass der Cloud-Anbieter Zugang zu den Informationen und Personendaten hat, sind die Geheimhaltungsvorgaben eingehalten. Zu diesen technischen Lösungen gehören die Verschlüsselung, bei welcher der Cloud-Anbieter keinen Schlüssel besitzt, sowie die Anonymisierung oder die Pseudonymisierung.

Wenn keine dieser technischen Lösungen eingesetzt werden kann, ist zu prüfen, ob die Geheimnispflichten die Auslagerung verunmöglichen. Bei Informationen und Personendaten, die unter dem Amtsgeheimnis stehen, sind die Mitarbeitenden des Cloud-Anbieters vertraglich in diese Geheimnispflicht einzubinden. Damit ist die Auslagerung möglich.

Beim Steuergeheimnis oder anderen besonderen Amtsgeheimnissen muss der Cloud-Anbieter die erhöhten Anforderungen an die Geheimhaltung einhalten können. Cloud-Anbieter im Ausland sind in einem Rechtsumfeld, das diesbezüglich nicht die notwendigen Garantien bietet. Das Gleiche trifft auf Anbieter zu, auf die der CLOUD Act anwendbar ist. In diesen Fällen dürfen Daten unter einem besonderen Amtsgeheimnis nicht ausgelagert werden, wenn keine technische Massnahme verhindert, dass der Cloud-Anbieter auf die Daten zugreifen kann.

Beim Steuergeheimnis oder anderen besonderen Amtsgeheimnissen muss der Cloud-Anbieter die erhöhten Anforderungen an die Geheimhaltung einhalten können.

Beim Berufsgeheimnis dürfen Informationen und Personendaten nur von der Geheimnisträgerin oder dem Geheimnisträger und ihren respektive seinen Hilfspersonen bearbeitet werden. Ausnahmen bestehen, wenn eine gesetzliche Bestimmung etwas anderes vorsieht, die betroffene Person im Einzelfall eingewilligt hat oder die vorgesetzte Behörde die Geheimnisträgerin oder den Geheimnisträger im Einzelfall von der Geheimnispflicht entbindet. Wenn die Mitarbeitenden des Cloud-Anbieters als Hilfspersonen qualifiziert werden können, besteht die Möglichkeit, auch Daten unter dem Berufsgeheimnis in die Cloud auszulagern. Bei Standardlösungen von internationalen Cloud-Anbietern sind ihre Mitarbeitenden in der Regel keine Hilfspersonen. Informationen und Personendaten unter dem Berufsgeheimnis können mit solchen Standardlösungen nur bearbeitet werden, wenn die Informationen verschlüsselt sind und das öffentliche Organ den Schlüssel behält oder wenn die Personendaten vorher anonymisiert oder pseudonymisiert wurden.

Die Geheimhaltungsvorgaben sind strafrechtlich abgesichert. Mitarbeitende von öffentlichen Organen können sich strafbar machen, wenn sie sich nicht an die Rahmenbedingungen halten (Art. 320 StGB oder Art. 321 StGB).

Verantwortung für die Datenbearbeitung wahrnehmen

Das öffentliche Organ bleibt auch bei der Auslagerung in die Cloud für die Daten verantwortlich. Es muss die Einhaltung des Datenschutzes gewährleisten und hat sicherzustellen, dass die Daten vom Cloud-Anbieter nur so bearbeitet werden, wie es das öffentliche Organ selbst auch tun darf. Diese Verantwortung wird einerseits durch vertragliche Regeln mit dem Cloud-Anbieter wahrgenommen. Der Regierungsrat erliess dafür die AGB Auslagerung Informatikleistungen und die AGB Datenbearbeitung durch Dritte. Die AGB sind für die kantonale Verwaltung verbindlich. Ihre Inhalte gelten für alle öffentlichen Organe des Kantons Zürich und sind in Verträgen mit Cloud-Anbietern einzubeziehen. Sie regeln zentrale Punkte zur Verantwortung für die Datenbearbeitung wie die Zweckbindung, den Umgang mit Unterauftragnehmern, das anwendbare Recht, den Gerichtsstand, bestimmte Massnahmen zur Informationssicherheit und die Kontrollmöglichkeiten.

Die öffentlichen Organe müssen andererseits angemessene organisatorische und technische Massnahmen treffen und von den Cloud-Anbietern einfordern. Dafür ist eine Risikobeurteilung vorzunehmen. Die Verschlüsselung spielt eine grosse Rolle als Massnahme zur Minderung der Risiken. Wenn Personendaten in Datenzentren in Ländern ohne gleichwertiges Datenschutzniveau bearbeitet oder gespeichert werden, müssen sie verschlüsselt werden und der Schlüssel muss beim öffentlichen Organ liegen. Wenn die Daten in Datenzentren im Inland oder in einem Land mit gleichwertigem Datenschutzniveau bearbeitet werden, müssen nur die besonderen Personendaten verschlüsselt werden. Der Schlüssel muss in diesen Fällen nur dann beim öffentlichen Organ liegen, wenn dies die Beurteilung der Risiken ergibt. Muss der Cloud-Anbieter aus operativen Gründen in Besitz des Schlüssels sein, muss er vertraglich verpflichtet werden, den Schlüssel nur auf explizite Anfrage und nach expliziter Einwilligung des öffentlichen Organs einzusetzen und nur dann auf die Daten zuzugreifen.

Spezialfall CLOUD Act

Der CLOUD Act ist ein Gesetz der USA. Es ermöglicht bestimmten US-Behörden, amerikanische Unternehmen zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, auch wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Der CLOUD Act ist ein Gesetz mit extraterritorialer Wirkung. Dieses Verfahren und dieser Zugriff auf Daten sind mit dem Datenschutzrecht und dem übergeordneten schweizerischen Recht nicht vereinbar. Es verstösst gegen den «ordre public» der Schweiz.

Wenn Personendaten, die einem besonderen Amtsgeheimnis oder einem Berufsgeheimnis unterstehen, an einen US-amerikanischen Cloud-Anbieter ausgelagert werden, darf der Anbieter keinen Zugang zu den Daten haben. Dies muss mit einer technischen Lösung sichergestellt werden, also durch Verschlüsselung, wobei der Schlüssel beim öffentlichen Organ verbleibt.

Wenn besondere Personendaten an einen US-amerikanischen Cloud-Anbieter ausgelagert werden, müssen technische Massnahmen umgesetzt werden, die eine Kenntnisnahme durch die US-Behörden unter dem CLOUD Act ausschliessen. Dies ergibt sich aus der Verantwortlichkeit des öffentlichen Organs. Die Kenntnisnahme kann durch eine Verschlüsselung ausgeschlossen werden, wobei der Schlüssel beim öffentlichen Organ verbleiben muss. Vertragliche Absicherungen genügen nicht, da der Anbieter die Gesetze der USA und damit die Bestimmungen des CLOUD Act befolgen muss.

Anonymisierte und pseudonymisierte Daten dürfen unverschlüsselt ausgelagert werden.

Besondere Risiken der Cloud

Zu den besonderen Risiken der Auslagerung in die Cloud gehört die ungenügende Transparenz über die Bearbeitung der Personendaten durch den Cloud-Anbieter – einschliesslich der Daten von Mitarbeitenden des öffentlichen Organs bei der Nutzung der Cloud-Anwendung. Die Einhaltung der Zweckbindung kann nicht richtig eingeschätzt werden. Weiter können der Auftraggeber und seine Aufsichtsbehörde den Cloud-Anbieter nur schwer kontrollieren. Weitere Risiken sind der Einfluss ausländischer Rechtsordnungen und Einschränkungen beim Datenschutz. Zudem sind die Daten in einem System eingeschlossen, die Portabilität der Daten und die Interoperabilität mit anderen Systemen also erschwert. Kontrollverlust, Datenverlust und Datenmissbrauch müssen auch in Betracht gezogen werden.

Zu den besonderen Risiken der Auslagerung in die Cloud gehört die ungenügende Transparenz über die Bearbeitung der Personendaten.

Datenschutz-Folgenabschätzungen für Cloud-Projekte

Öffentliche Organe müssen für beabsichtigte Bearbeitungen von Personendaten eine Datenschutz-Folgenabschätzung (DSFA) erstellen. Bei Cloud-Projekten ist dies besonders wichtig, da die Auslagerung in die Cloud erhöhte Risiken mit sich bringt. Die Datenschutzbeauftragte stellt für die DSFA auf ihrer Website ein Formular *(https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung)* zur Verfügung. Darin müssen die Risiken des Projekts für die Grundrechte der betroffenen Personen aufgezeigt werden. Gleichzeitig sind angemessene organisatorische und technische Massnahmen zu beschreiben, durch die die Risiken reduziert werden sollen. Wenn besondere Risiken für die Grundrechte vorliegen, muss das Projekt vorab der Datenschutzbeauftragten zur Prüfung unterbreitet werden. Nur eine DSFA gibt dem öffentlichen Organ die Möglichkeit, die konkreten Risiken des Cloud-Projekts einzuschätzen und angemessen mit ihnen umzugehen.

Noch keine Vorabkontrollen zu Microsoft 365

Bei der Einführung von Microsoft 365 muss in vielen Fällen von besonderen Risiken für die Grundrechte der betroffenen Personen ausgegangen werden. In diesen Fällen ist das Projekt der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten. Dafür müssen die Beschreibung des Projekts, die Darstellung der Rechtslage und eine Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen eingereicht werden. Dazu gehören die DSFA und das ISDS-Konzept. Bisher reichte jedoch noch kein öffentliches Organ im Kanton Zürich der Datenschutzbeauftragten ein Projekt zur Einführung von Microsoft 365 zur Vorabkontrolle ein.

Drang der Spitäler in die Cloud

Auch bei Anfragen von Spitälern steht die Anwendung Microsoft 365 im Vordergrund. Die Datenschutzbeauftragte beriet auch zu anderen Anwendungen. Spitäler bearbeiten praktisch immer Daten, die dem Berufsgeheimnis unterstehen und besondere Personendaten darstellen, weil sie Informationen über die Gesundheit enthalten.

Der Schritt in die Cloud hängt bei Spitälern von technischen Lösungen ab, die verhindern, dass der Cloud-Anbieter Zugriff auf die Daten bekommt. Die Spitäler müssen ihre Daten in der Cloud verschlüsseln und im Besitz des Schlüssels bleiben.

Bei der Auslagerung in die Cloud müssen Spitäler die Kenntnisnahme der Daten ihrer Patientinnen und Patienten durch Unbefugte in jedem Fall durch eine technische Lösung verhindern.

Anonymisierte oder pseudonymisierte Daten können unverschlüsselt ausgelagert werden. Bei pseudonymisierten Daten dürfen der Cloud-Anbieter oder andere mögliche Empfängerinnen und Empfänger keinen Zugang zum Schlüssel der Pseudonymisierung haben. Sie dürfen auch nicht über andere Kenntnisse verfügen, um die Daten wieder einer bestimmten Person zuordnen zu können.

Nicht alle Daten im Gesundheitsbereich können pseudonymisiert werden, weil viele Daten die Bestimmtheit in sich tragen und nur einer Person zugeordnet werden können. Dies betrifft beispielsweise genetische Daten. Bei der Auslagerung in die Cloud müssen Spitäler die Kenntnisnahme der Daten ihrer Patientinnen und Patienten durch Unbefugte in jedem Fall durch eine technische Lösung verhindern.

Hochschulinstitut Psychologie und Microsoft 365

Ein Hochschulinstitut der Psychologie wandte sich im Zusammenhang mit Microsoft 365 an die Datenschutzbeauftragte. Das Institut verfügt über Daten, die dem Berufsgeheimnis unterstehen.

Die zuständigen Personen des Instituts waren nicht sicher, ob sie diese Daten mit Microsoft 365 in der Cloud bearbeiten dürfen. Die Datenschutzbeauftragte wurde auf die Website der zentralen Informatik der Hochschule hingewiesen, wo die Nutzung von Microsoft 365 für Personendaten, die dem Berufsgeheimnis unterstehen, erlaubt wird. Es müsse der Zusatzdienst einer Kunden-Lockbox eingesetzt werden.

Kundinnen und Kunden können mit der Kunden-Lockbox von Microsoft 365 den Zugriff von Microsoft-Mitarbeitenden bei Support- und Wartungsfällen steuern. Mit der zusätzlichen Funktion der Kunden-Lockbox kann ihr Zugriff eingeschränkt werden. Wenn Mitarbeitende von Microsoft zu Support- und Wartungszwecken auf die Daten zugreifen wollen, müssen sie vorher die Auftraggeberin oder den Auftraggeber ausdrücklich um Genehmigung fragen.

Daten, die dem Berufsgeheimnis unterstehen, dürfen nicht in die Cloud von Microsoft ausgelagert werden, auch nicht mit der Kunden-Lockbox.

Der Schutz der Kunden-Lockbox kommt nicht zur Anwendung, wenn eine US-Behörde von Microsoft Zugriff auf Daten ihrer Kundinnen und Kunden verlangt und sich dabei auf den CLOUD Act stützt. Daten, die dem Berufsgeheimnis unterstehen, dürfen deshalb nicht in die Cloud von Microsoft ausgelagert werden, auch nicht mit der Kunden-Lockbox.

Nicht alles, was praktisch ist, ist auch erlaubt

Seit 2021 besteht im Kanton Zürich eine Bienenfachstelle. Sie erarbeitet und koordiniert Massnahmen zur Förderung der Honig- und Wildbienen und stellt Informationen dazu bereit. Der Auftrag zur Führung der Bienenfachstelle ging für drei Jahre an eine Interessengemeinschaft von Bienenfreundinnen und Bienenfreunden. Auf der einen Seite steht die Begeisterung für das Thema, auf der anderen Seite stehen die Vorgaben des öffentlichen Rechts.

Die Datenschutzbeauftragte führte drei Beratungen durch zur Tätigkeit der Bienenfachstelle, die miteinander zusammenhingen. Sie zeigten die Herausforderungen auf, die sich daraus ergeben, wenn eine private Interessengemeinschaft staatliche Aufgaben übernimmt.

Die Bienenfachstelle verlangte von einem kantonalen Amt die Informationen über Bienenvölker und die Standorte der Bienenstände. Das Amt zögerte mit der Herausgabe, weil die Sachinformationen mit Personendaten verknüpft waren. Die Bienenfachstelle wandte sich darauf an die Datenschutzbeauftragte. Andererseits wandten sich Privatpersonen aus Imkerkreisen an die Datenschutzbeauftragte, weil die Bienenfachstelle Namen und Adressen der Imkerinnen und Imker sowie weitere Informationen zu ihrer Tätigkeit über den GIS-Browser im Internet veröffentlichen wollte.

Die Bekanntgabe von Personendaten im GIS-Browser und damit im Internet ist nicht notwendig, damit die Bienenfachstelle ihre Aufgabe erfüllen kann. Sie ist deshalb auch nicht erlaubt.

Ein privater Verein, der im Rahmen eines Auftrags öffentliche Aufgaben erfüllt, gilt als öffentliches Organ im Sinne des Gesetzes über die Information und den Datenschutz. Deshalb kann die Interessengemeinschaft für die Tätigkeit der Bienenfachstelle Amtshilfe in Anspruch nehmen, jedoch nur im Einzelfall und nur, wenn es die Informationen benötigt, um die Aufgabe erfüllen zu können. Die Bearbeitung von Personendaten ist zulässig, wenn eine rechtliche Grundlage vorliegt und sie für die Zweckerreichung geeignet und erforderlich und somit verhältnismässig ist.

Die Integration der Informationen im GIS-Browser könnte praktisch sein, um schnell einen Überblick über die Standorte der Bienenvölker und weitere Informationen zu bekommen. Die Bekanntgabe im Internet ist jedoch nicht notwendig, damit die Bienenfachstelle ihre Aufgabe erfüllen kann. Sie ist deshalb auch nicht erlaubt.

Allerdings wies die Datenschutzbeauftragte darauf hin, dass Personendaten im GIS-Browser nicht für die Öffentlichkeit freigeschaltet werden müssen. Sie können auch nur einem engeren Nutzerkreis mit spezieller Berechtigung zugänglich gemacht werden.

Biometrische Auswertung beim Online-Assessment

Eine Direktion legte der Datenschutzbeauftragten das Projekt für den Einsatz von Online-Assessments bei der Personalrekrutierung vor. Während das Assessment absolviert wird, werden Bildaufnahmen gemacht und automatisch ausgewertet.

Bei Unregelmässigkeiten werden die Recruiterin oder der Recruiter darüber informiert und die Bildaufnahmen werden zugänglich gemacht. Das Assessment wird von den Stellenbewerbenden in den meisten Fällen in ihren Privaträumen absolviert. Das Bildmaterial wird biometrisch ausgewertet. Dadurch soll sichergestellt werden, dass die Bewerberin oder der Bewerber das Assessment selbst durchführt und keine zusätzliche Person mithilft.

Die Datenschutzbeauftragte beurteilte die Bildaufnahmen und ihre biometrische Auswertung als unverhältnismässig für den Zweck der Verhinderung von unlauterem Verhalten. Sie hält fest, dass mildere Mittel einzusetzen sind. Zudem verlangt sie, dass die Daten in Zusammenhang mit dem Assessment verschlüsselt gespeichert werden. Sie sollen gelöscht werden, sobald der Zweck der Rekrutierung erfüllt ist.

Verhältnismässigkeit bei Online-Prüfungen

Während der Corona-Pandemie mussten Schulen und Hochschulen die Prüfungen oft online durchführen. Zur Beaufsichtigung der Prüflinge wurde Überwachungssoftware eingesetzt. Für Aufmerksamkeit sorgte der Einsatz der Software Proctorio. Klar ist: Überwachungssoftwares sind gekommen, um zu bleiben. Die Datenschutzbeauftragte hat den Einsatz in einer Hochschule mit Vorabkontrollen geprüft.

Wenn eine Hochschule Prüfungen durchführt, muss sie die redliche und rechtsgleiche Durchführung überwachen können. Nicht nur bei Online-Prüfungen leistet hier Proctoring-Software gute Dienste. Auch bei Prüfungen vor Ort werden Funktionen wie das Übertragen der Bildschirmaktivität eingesetzt. Der gesetzliche Lehrauftrag ist die Rechtsgrundlage für diese Bearbeitung von Personendaten.

Die Softwares bieten eine grosse Anzahl Funktionen an. Diese greifen unterschiedlich stark in die Privatsphäre der Studierenden ein. Deshalb ist die Verhältnismässigkeit der verwendeten Funktionen abzuklären.

Die Datenschutzbeauftragte beurteilte den Einsatz der Sperrfunktionen als zumutbar. Die Sperrfunktion des Produkts Proctorio schränkt die Nutzung des Browsers während der Prüfung ein. So kann beispielsweise der Vollbildmodus erzwungen oder Downloads können blockiert werden. Damit kann bei Fernprüfungen wie bei Prüfungen vor Ort unredliches Verhalten besser erfasst werden als mit bisherigen Möglichkeiten.

Die angebotenen Funktionen greifen unterschiedlich stark in die Privatsphäre der Studierenden ein. Deshalb ist die Verhältnismässigkeit der verwendeten Funktionen abzuklären.

Eine weitere Funktion ermöglicht, die Bildschirminhalte der Prüflinge aufzuzeichnen und automatisch auszuwerten. Noch weitergehend können auch Audio und Video aufgezeichnet und automatisch ausgewertet werden. Dabei werden beispielsweise die Kopfbewegungen der Prüflinge analysiert oder es soll erkannt werden, ob mehrere Personen im Raum sind.

Die Datenschutzbeauftragte beurteilt die Aufzeichnung und Auswertung von Bild und Ton als nicht zumutbar. Die Funktionsweise der Algorithmen ist für die Studierenden intransparent. Dies kann dazu führen, dass sie ihr Verhalten aus Unsicherheit ändern, auch wenn dies nicht nötig wäre. Ihr Einsatz ist nicht verhältnismässig.

Die Datenschutzbeauftragte beurteilt hingegen die Aufzeichnung und Auswertung der Bildschirminhalte als verhältnismässig. Sie geht aufgrund der Beschreibungen der Funktion davon aus, dass sie geeignet ist, um bestimmte Unredlichkeiten festzustellen. Sie sind bedeutend weniger starke Eingriffe in die Privatsphäre als die Aufzeichnung und die Auswertung von Bild und Ton aus den Privaträumen der Studierenden.

Die Aufzeichnung der Bildschirminhalte sind bedeutend weniger starke Eingriffe in die Privatsphäre als die Aufzeichnung und Auswertung von Bild und Ton aus den Privaträumen der Studierenden.

Die Hochschule listet im Reglement Fernprüfungen die möglichen Prüfungsarten auf. Sie ordnet die Prüfungsarten nach der Intensität des Eingriffs in die Privatsphäre der Studierenden. Die digitale Prüfung ohne Proctoring greift am wenigsten in die Privatsphäre ein, die digitale Prüfung mit Aufzeichnung am stärksten. Die Prüfungsverantwortlichen schätzen bei jeder Prüfung die Verhältnismässigkeit ein und wählen die entsprechende Prüfungsart aus. Die Datenschutzbeauftragte beurteilt die Einordnung der Eingriffsintensität und die Zuweisung der Entscheidung an die Prüfungsverantwortlichen als korrekt. Die Studiengangleitenden verfügen über die nötige Nähe zur Sache, um die Verhältnismässigkeit einzuschätzen.

Auslagerung in die Cloud

Proctoring-Software ist meistens als Software as a Service konzipiert. Der Anbieter betreibt die Software auf einer Cloud-Plattform wie Microsoft Azure. Diese Cloud-Anbieter stellen Unterauftragnehmer des öffentlichen Organs dar. Das öffentliche Organ ist dafür verantwortlich, dass die Verpflichtungen des Auftragnehmers auch vom Unterauftragnehmer eingehalten werden. Solche Konstellationen erschweren die Übersicht. Eine effektive Kontrolle über die Einhaltung von Informationssicherheitsstandards ist kaum mehr möglich.

Informationssicherheit bei Gemeinden stärken

Gemeinden sind ein beliebtes Ziel für Cyberkriminelle. Besonders kleinere Gemeinden verfügen kaum über genügend Fachpersonen aus Datenschutz und Informationssicherheit. Die Datenschutzbeauftragte unterstützt sie mit praxisnahen Vorlagen sowie Merkblättern im Rahmen eines Datenschutzreviews mit Selbstdeklaration.

Im Kanton Zürich gibt es 160 Gemeinden. Davon haben 87 weniger als 6000 Einwohnerinnen und Einwohner. Sie stehen in Sachen Datenschutz und Informationssicherheit vor denselben Herausforderungen wie grosse Gemeinden, allerdings mit viel weniger personellen und finanziellen Ressourcen. Zudem sind Datenschutzreviews im herkömmlichen Sinn nicht nur für die Gemeinden sehr zeitaufwendig. Die Ressourcen der Datenschutzbeauftragten reichten nicht aus, um alle Gemeinden in sinnvollen Abständen zu kontrollieren.

Deshalb entwickelte die Datenschutzbeauftragte den Datenschutzreview mit Selbstdeklaration. Sie stellt den Gemeinden praxisnahe Hilfsmittel zur Verfügung. Dazu gehören Vorlagen für ein Berechtigungskonzept, ein Plan für die Sensibilisierung der Mitarbeitenden oder ein Notfallkonzept. Damit können sich die Gemeinden einen Überblick über ihre IKT-Infrastruktur verschaffen, diese selbst beurteilen und verbessern sowie die Informationssicherheitsmassnahmen einfach dokumentieren. Dadurch kann mit möglichst geringem Aufwand ein professioneller Grundschutz für die Personendaten erreicht werden.

Nach einer Einführung vor Ort durch eine Mitarbeitende oder einen Mitarbeitenden der Datenschutzbeauftragten aus der Abteilung Informationssicherheit erstellen die Gemeinden alle notwendigen Konzepte, Inventare und Richtlinien selbst anhand der Vorlagen und Hilfestellungen. Die Fachpersonen der Datenschutzbeauftragten stehen beratend zur Seite und beantworten Fragen. Anschliessend prüft die Datenschutzbeauftragte die Dokumente und stellt der Gemeinde einen Bericht aus.

Die Datenschutzbeauftragte maximiert die Wirksamkeit der vorhandenen Ressourcen und stärkt die Informationssicherheit und den Datenschutz flächendeckend.

Der Datenschutzreview mit Selbstdeklaration ermöglicht die gleichzeitige Betreuung vieler Gemeinden. Die Datenschutzbeauftragte maximiert so die Wirksamkeit der vorhandenen Ressourcen und stärkt die Informationssicherheit und den Datenschutz flächendeckend. Seit der Lancierung im Jahr 2021 haben 21 Gemeinden einen solchen Review begonnen. Fünf Datenschutzreviews mit Selbstdeklaration konnten abgeschlossen werden. Im Jahr 2023 wird die Datenschutzbeauftragte weitere 30 Gemeinden zur Selbstdeklaration einladen.

Besonderer Schutz für religiöse Aktivitäten

Die Datenschutzbeauftragte wird immer wieder gefragt, welches Datenschutzgesetz für die Kirchgemeinden anwendbar ist. Auch Vereine mit karitativen Zwecken möchten wissen, welche Bestimmungen für sie gelten. Auch die Voraussetzungen bei der Bekanntgabe und die Zweckbindung sind immer wieder Thema in der Beratung.

Das Kirchengesetz hält fest, dass die Evangelisch-reformierte Landeskirche, die Römisch-katholische Körperschaft und die Christkatholische Kirchgemeinde zu den kantonalen kirchlichen Körperschaften zählen. Das Gesetz über die anerkannten jüdischen Gemeinden erwähnt die Israelitische Cultusgemeinde Zürich sowie die Jüdische Liberale Gemeinde. Für die Datenbearbeitungen durch diese Religionsgemeinschaften ist somit das IDG anwendbar.

Kirchgemeinde gibt Adressen an Verein

Ein Verein mit karitativem Zweck verschickte bis anhin seine Jahresberichte an die Adressen, die er von der Kirchgemeinde erhalten hatte. Ein Empfänger beschwerte sich über diese Praxis. Der Verein bat die Datenschutzbeauftragte, die Rechtslage zu beurteilen. Für eine Bekanntgabe von Daten verlangt das Gesetz über die Information und den Datenschutz eine gesetzliche Grundlage oder die Einwilligung der Betroffenen, unabhängig davon, ob es sich um einfache Personendaten oder sensitive Informationen, wie religiöse Daten, handelt. Die datenschutzrechtlichen Bestimmungen beim Bezug von Adressen von den Kirchgemeinden sind einzuhalten, auch wenn Vereine karitative Arbeit verrichten und geltend machen, auf Adressdaten angewiesen zu sein. Die Weitergabe der Adressen durch die Kirchgemeinde an den Verein war nicht rechtmässig. In diesem Fall bieten sich andere Lösungen an. Die Kirchgemeinde kann die Betroffenen um Einwilligung zur Bekanntgabe der Adressen an den Verein anfragen oder sie kann die Jahresberichte selbst verschicken.

Die datenschutzrechtlichen Bestimmungen beim Bezug von Adressen von den Kirchgemeinden sind einzuhalten, auch wenn Vereine karitative Arbeit verrichten.

Meinungsforschung nach Kirchenaustritt

Eine Kirchgemeinde wollte die Datensätze der austretenden Mitglieder einem Meinungsforschungsinstitut zur Verfügung stellen. In einer telefonischen Befragung sollten die Austrittsgründe zusammengetragen werden. Das Kirchengesetz hält fest, dass Austrittsgespräche geführt werden dürfen. Die Kirchgemeinde darf auch Dritte damit beauftragen. Es handelt sich um eine Auslagerung. Die Kirchgemeinde bleibt für die Datenbearbeitung verantwortlich. Deshalb muss ein schriftlicher Vertrag abgeschlossen werden, in dem die Bestimmungen des Gesetzes über die Information und den Datenschutz an das Meinungsforschungsinstitut übertragen werden. Das Meinungsforschungsinstitut darf die Daten nur so bearbeiten, wie es die Kirchgemeinde auch dürfte. Es gilt das Zweckbindungsgebot. Der Leitfaden Bearbeiten im Auftrag *(https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf)* hilft beim Vorgehen.

E-Mobilität

Eine Landeskirche möchte die nachhaltige Mobilität in den Pfarreigemeinden fördern. Dazu erstellte sie ein Konzept zur E-Mobilität. Den Gemeinden sollen E-Bikes, E-Cargo-Bikes und Ladestationen zur Verfügung gestellt werden. Die Nutzung soll danach evaluiert werden.

Vom Einsatz eines Umfragetools eines US-Unternehmens ist in diesem Fall abzusehen. Die hier bearbeiteten Personendaten sind in jedem Fall besondere Personendaten, da sie in Zusammenhang mit einer religiösen Aktivität stehen. Das Bearbeiten der Daten im Ausland sollte aufgrund der hohen Risiken unterlassen werden.

Die Datenschutzbeauftragte wies darauf hin, bei der Evaluation darauf zu achten, dass keine Rückschlüsse auf einzelne Personen möglich sind. Wenn die Nutzung beispielsweise nach gleichem Aufgabenfeld aufgeschlüsselt wird, kann aufgrund der geringen Anzahl an Teilnehmenden auf Personen rückgeschlossen werden. Die Entfernung von Namen führt also nicht zur Anonymisierung der Daten.

Microsoft 365 in Kirchgemeinden

Die Bestimmungen des IDG gelten auch bei der Cloud-Nutzung. Auch Kirchgemeinden setzen zunehmend Microsoft 365 ein. Hier gelten dieselben Anforderungen wie in der kantonalen oder kommunalen Verwaltung. Allerdings sind Informationen zu religiösen Aktivitäten immer besondere Personendaten und müssen zusätzlich geschützt werden. Deshalb ist der Risikoanalyse vor dem Einsatz von Microsoft 365 besondere Beachtung zu schenken. Der Leitfaden Nutzung externer Cloud-Dienste *(https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_nutzung_externer_cloud_dienste.pdf)* führt Schritt für Schritt durch die verschiedenen Phasen der Evaluation der Cloud-Dienste und beschreibt die Möglichkeit ihres Einsatzes. Es ist eine Datenschutz-Folgenabschätzung durchzuführen und das Projekt ist bei der Datenschutzbeauftragten zur Vorabkontrolle einzureichen.

Datenschutzreglemente

Eine Kirchgemeinde legte der Datenschutzbeauftragten ihr Datenschutzreglement vor. Als öffentliche Organe müssen sich Kirchgemeinden bei der Datenbearbeitung an die gesetzlichen Grundlagen halten. Ein Datenschutzreglement ist deshalb nicht notwendig. Es kann allerdings dazu beitragen, die Mitarbeitenden im Umgang mit Informationen zu religiösen Aktivitäten sicherer zu machen.

Mehr zur «Auslagerung in die Cloud: Risiken und Regeln» *(https://www.datenschutz.ch/tb/2022/risiken-und-regeln)*

Mehr Lebensqualität

Was kann mir schon passieren? Über mich ist alles bekannt. Mit diesem Motto rief die Datenschutzbeauftragte zur Teilnahme am siebten Datenschutz-Video-Wettbewerb auf. Die Gewinnervideos überzeugen durch ihre Machart, die technische Umsetzung und die allgemein hochstehende Qualität.

Mit dem ersten Preis ausgezeichnet wurde «Gemeinsam für die Privatsphäre. Damit du mehr Zeit zum Fussball spielen hast.», ein überraschender Kurzfilm von Andrina Schmid, Samuel Wetter und Benjamin Dangel.

100 Sekunden reichen dem Macherteam des Gewinnervideos. Es zeigt, welche Lebensqualität wir verlieren, weil zu viel von uns bekannt ist. Der Protagonist des Videos heisst Max und er liebt Fussball. Eigentlich liebt er es vor allem, Fussball zu spielen. Je mehr Zeit er im Internet verbringt, desto mehr Informationen werden über ihn gesammelt. Das ist bekannt. Je mehr Informationen die Internetfirmen über Max haben, desto besser werden sie darin, ihn dazu zu verleiten, noch länger online zu sein. Was Max am Schluss fehlt, ist die Zeit für das, was er eigentlich am liebsten tut – Fussballspielen eben. Das ist Max. Das Video macht aber klar: Das passiert uns allen. Die Datenschutzbeauftragte lobte den Beitrag an der Preisverleihung im Zürcher Kino RiffRaff: «Das Video nimmt in gelungener, überraschender und origineller Art und Weise Bezug auf das Thema des Wettbewerbs. Es ist sehr kurzweilig und mit vielen Infos vollgepackt, so dass man es gerne auch ein zweites Mal anschauen will.»

100 Sekunden reichen dem Macherteam des Gewinnervideos. Es zeigt, welche Lebensqualität wir verlieren, weil zu viel von uns bekannt ist.

Zum zweitplatzierten Beitrag «Don't wait» von Phil Jaycob sagte das Jurymitglied Flurin Senn, Medienpädagoge der Pädagogischen Hochschule Zürich: «Hier beherrscht jemand die hohe Kunst, eine Aussage ohne Monolog oder Dialog in Bild zu bringen. Das Video überzeugt durch eine gute und logische Führung der Zuschauerinnen und Zuschauer.» Das Video zeigt, welchen Unterschied ein einziger Klick im Leben ausmachen kann, wenn bei einem dieser nervigen Pop-ups, die auf ein Software-Update hinweisen, «Später» statt «Jetzt installieren» gewählt wird.

Mit dem dritten Preis ausgezeichnet wurde der kurze Spielfilm «Was kann mir schon passieren?» von Jannick Glück, Reto Gfeller und Christoph Rahm. Er thematisiert die Problematik der Filterblasen und ihrem Potenzial zur Spaltung unserer Gesellschaft. Jurymitglied Nadia Holdener, Videomaker und Lehrbeauftragte Audiovisual/Cast an der Zürcher Hochschule der Künste (ZHdK), betonte in ihrer Laudatio, dass der Beitrag eine gesellschaftlich relevante Botschaft auf sehr vergnügliche Weise und in einem Alltagsszenario aufarbeite.

Weitere Videos und Informationen gibt es in der Mitteilung «Prämierte Videos werfen vielfältigen Blick auf die Bedeutung der Privatsphäre» *(https://www.datenschutz.ch/mitteilungen/2022/was-kann-mir-schon-passieren-datenschutz-video-wettbewerb-2022)*.

Mehr Wissen sorgt für besseren Datenschutz

Wer unsicher ist, macht mehr Fehler. Das gilt auch für den Umgang mit dem Datenschutz und der Informationssicherheit. Beide Themen betreffen alle Mitarbeitenden öffentlicher Organe ganz besonders. Die Datenschutzbeauftragte sorgt für mehr Wissen mit der neuen Lernumgebung lerne.datenschutz.ch *(https://lerne.datenschutz.ch/)*

Für die meisten Mitarbeitenden öffentlicher Organe gehören Datenschutz und Informationssicherheit nicht zu den Kernaufgaben. Trotzdem sind sie verantwortlich für die Einhaltung und die Umsetzung der Vorschriften und Anforderungen. Die Datenschutzbeauftragte hat zusammen mit der Pädagogischen Hochschule Bern eine neue Online-Lernumgebung erstellt.

Auf spielerische Weise kann das Wissen über die Grundsätze und Anforderungen getestet werden, wie sie im Gesetz über die Information und den Datenschutz definiert sind. Zusätzlich werden in kurzen Animationsvideos aktuell drei Fallbeispiele aus der Beratungspraxis der Datenschutzbeauftragten präsentiert. Hier können die Datenschutz-Herausforderungen herausgefunden werden, die in diesen Beispielen versteckt sind. Zudem können Fehler entdeckt werden und das richtige Vorgehen in diesen Situationen kann geübt werden.

Die Lernumgebung lerne.datenschutz.ch *(https://lerne.datenschutz.ch/)* wird laufend erweitert. So können spezifische Module für verschiedene Themenbereiche oder Fachgebiete zur Verfügung gestellt werden.

Praktische Tipps für die Digitalisierung in der Verwaltung

Die Datenschutzbeauftragte führte in Zusammenarbeit mit der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) die 1. Zürcher Datenschutztagung durch. Die teilnehmenden Mitarbeitenden öffentlicher Organe bekamen konkrete Handlungsanleitungen für eine erfolgreiche datenschutzkonforme Digitalisierung in Kantons- und Gemeindeverwaltungen sowie Schulen.

Über die Digitalisierung in öffentlichen Organen wurde schon viel diskutiert. Oft wurde der Mangel an Digitalisierung kritisiert. Selten bekamen die verantwortlichen Mitarbeitenden konkrete und praktische Handlungsanleitungen und Tipps, wie sie vorgehen sollen. Mit der Zürcher Datenschutztagung wollen die Datenschutzbeauftragte und die ZHAW diesen Mangel beheben.

In der ersten Durchführung im September 2022 konnten die 74 Teilnehmenden von drei Referaten profitieren. Der stellvertretende Beauftragte für Information und Datenschutz des Kantons Solothurn, Julian Powell, verschaffte einen Überblick der besonderen Herausforderungen, die die Digitalisierung an die Verwaltung stellt. Die Datenschutzbeauftragte des Kantons Zürich Dominika Blonski zeigte die Vorgehensweisen für eine erfolgreiche Digitalisierung auf. Nadja Braun Binder, Professorin für öffentliches Recht an der Universität Basel, stellte die Möglichkeiten des Einsatzes Künstlicher Intelligenz in öffentlichen Organen vor.

Oft wurde der Mangel an Digitalisierung in öffentlichen Organen kritisiert. Selten bekamen die verantwortlichen Mitarbeitenden konkrete und praktische Handlungsanleitungen und Tipps.

Am Nachmittag wurden drei Workshops angeboten. Die Teilnehmenden bekamen die Möglichkeit, ihre Anliegen mit drei Experten zu bearbeiten. Die Datenschutzbeauftragte stellt auf ihrer Website einen grossen Schatz an Informationen und Hilfsmitteln zur Verfügung, auch zur Entscheidungshilfe für den Einsatz digitaler Tools. Ihr Abteilungsleiter Recht, Jörg Eckardt, zeigte, wie beispielsweise die Checkliste im Leitfaden Bearbeiten im Auftrag gute Dienste leistet. Dies an einem Fallbeispiel aus der Beratungspraxis. Marcel Griesinger, Dozent der ZHAW, erarbeitete anhand des Leitfadens zur Informationssicherheit in Volksschulen, herausgegeben und publiziert durch die Datenschutzbeauftragte des Kantons Zürich, einen Überblick zur Umsetzung einer nachhaltigen Informationssicherheit. Mit Bernhard Stüssy, stellvertretender Abteilungsleiter Überlieferungsbildung des Staatsarchivs, wurden die datenschutzrechtlichen Aspekte bei der digitalisierten Archivierung eruiert.

Die Datenschutzbeauftragte bot spezifisch angepasste Weiterbildungen an für unterschiedliche Zielgruppen.

Insgesamt führte die Datenschutzbeauftragte 29 Weiterbildungen durch. Dazu gehörten Beiträge zu den CAS Datenschutzverantwortliche, CAS Sozialhilfe und CAS Kindes- und Erwachsenenschutzrecht (KESR) an der ZHAW.

Die Datenschutzbeauftragte bot spezifisch angepasste Weiterbildungen an für unterschiedliche Zielgruppen. Sie trug mit einem Referat zu Datenschutz in der Einwohnerkontrolle zum Fachseminar des Verbands Zürcher Einwohnerkontrollen bei. Lernende der öffentlichen Verwaltung in kaufmännischer Ausbildung bekamen eine Einführung in die Themen Amtsgeheimnis und Datenschutz. Die Datenschutzbeauftragte unterstützte eine Kindes- und Erwachsenenschutzbehörde mit einer Fallbesprechung und vertieften Informationen zur Verbesserung der Informationssicherheit.

Im Jahr 2022 publizierte der Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV) das E-Book «Kompetent in Behörde und Verwaltung». Die Datenschutzbeauftragte trug das Fachkapitel Datenschutz zu dieser Publikation bei.

Selbstbestimmt digital unterwegs dank reflektierter Grundhaltung

Der zweite Band des preisgekrönten Lehrmittels «Selbstbestimmt digital unterwegs» ist erschienen. Unter dem Titel «Meine Daten, meine Spuren» sind vier Lektionen für die 9- bis 13-jährigen Schülerinnen und Schüler des Zyklus 2 des Lehrplans 21 zusammengefasst. Die ganze Lehrmittelreihe ist kostenlos verfügbar unter www.datenschutzlernen.ch *(https://www.datenschutzlernen.ch/)*.

2019 lancierten die Datenschutzbehörde des Kantons Zürich und die Pädagogische Hochschule Zürich gemeinsam eine Weltneuheit: «Geheimnisse sind erlaubt», ein Datenschutz-Lehrmittel für 4- bis 8-jährige Kinder. Es wurde von der Internationalen Konferenz der Datenschutzbeauftragten mit dem Global Privacy and Data Protection Award ausgezeichnet. Nun ist der zweite Teil des Lehrmittels kostenlos online zugänglich. In «Meine Daten, meine Spuren» werden vier Unterrichtseinheiten für den Zyklus 2 des Lehrplans 21 bereitgestellt.

«Meine Daten, meine Spuren» setzt in einem Alter an, in dem Kinder erstmals selbstständig das Internet und soziale Medien erkunden. In «Geheimnisse sind erlaubt» wird Kindern am Beispiel von alltäglichen Geheimnissen das Konzept von Privatsphäre und Datenschutz vermittelt. Darauf aufbauend findet im Lehrmittel für den Zyklus 2 verstärkt ein Übergang in die digitale Welt statt. Die Schülerinnen und Schüler setzen sich auf spielerische und kreative Weise mit Themen wie Videoüberwachung, Onlinewerbung und Privatsphäre im Internet auseinander.

Es wird bewusst nicht auf technisches Wissen und toolbezogene Fähigkeiten fokussiert, da sich die technischen Herausforderungen in Zeiten der Digitalisierung rasant verändern.

Gespräche, Rollenspiele und gegenseitiger Austausch dienen als zentrale methodische Elemente. Es wird bewusst nicht auf technisches Wissen und toolbezogene Fähigkeiten fokussiert, da sich die technischen Herausforderungen in Zeiten der Digitalisierung rasant verändern. Die Schülerinnen und Schüler sollen vielmehr eine reflektierte Grundhaltung entwickeln, die ihnen ein selbstbestimmtes Leben in der digitalisierten Welt ermöglicht.

Die handlungsorientierten Lerneinheiten können von Lehrpersonen auch ohne spezielle Vorkenntnisse und ohne mediale Ausstattungen in den Unterricht integriert werden. Sie basieren auf den Best-Practice-Richtlinien des Arcades Project der Europäischen Union. Bezüge zu den Kompetenzen des Lehrplans 21 sind am Ende der einzelnen Unterrichtseinheiten aufgelistet.

Zu den Lehrmitteln auf www.datenschutzlernen.ch *(https://www.datenschutzlernen.ch/)*

Das Video auf dieser Seite ist auf der datenschutzkonformen, schweizerischen Videoplattform Switchtube veröffentlicht, weshalb keine Zwei-Klick-Lösung eingesetzt werden muss.

ZKB, neue AGB und die Aufsicht der DSB

Anfang des Jahres 2022 verschickte die Zürcher Kantonalbank (ZKB) ihre neuen Allgemeinen Geschäftsbedingungen (AGB). Ihr Inhalt führte zu verschiedenen Anfragen bei der Datenschutzbeauftragten von verunsicherten Privatpersonen. Die AGB erwähnten die Möglichkeit der Bank, Geschäftsbereiche und Dienstleistungen ganz oder teilweise auszulagern – auch ins Ausland.

Die ZKB ist eine selbstständige Anstalt des kantonalen Rechts. Sie steht im wirtschaftlichen Wettbewerb und handelt nicht hoheitlich. Sie untersteht deshalb nicht den Bestimmungen des Gesetzes über die Information und den Datenschutz (IDG). Die Datenschutzbeauftragte ist seit Juni 2020 für die Aufsicht über die Datenbearbeitungen der ZKB zuständig. Sie wendet das Bundesgesetz über den Datenschutz (DSG) an.

Die ZKB fällt im DSG unter die Bestimmungen für private Personen. Sie darf Personendaten bearbeiten, wenn sie bei den betroffenen Personen die Einwilligung einholt. Dies hat die ZKB mit dem Versand der AGB getan. Die damit transparent gemachten Datenbearbeitungen sind deshalb aus datenschutzrechtlicher Sicht rechtmässig (Art. 4 Abs. 5 DSG Bund und Art. 13 Abs. 1 DSG).

Die ZKB muss sich aber an die Sorgfaltspflichten halten, die in der Bankenbranche üblich sind.

Übermässige Datenbearbeitung

Das Handelsregisteramt stellt die Belege zu Handelsregistereinträgen seit 2012 im Internet zur Verfügung. Diese Bezugsmöglichkeit ist kostenlos, ohne Interessennachweis und von überall auf der Welt möglich. Mehrere Personen gelangten an die Datenschutzbeauftragte. Sie hatten festgestellt, dass die öffentlich zugänglichen Belege auch Informationen enthalten, die mit dem Handelsregistereintrag nichts zu tun hatten.

So waren beispielsweise Protokolle abrufbar, die nicht nur den Registereintrag belegten, sondern auch andere Beschlüsse enthielten. Sie stellten beim Handelsregisteramt Anträge, die nicht relevanten Inhalte der Belege zu schwärzen. Das Handelsregisteramt teilte ihnen mit, Belege dürften nachträglich nicht verändert werden.

Die Handelsregister sind öffentliche Register des Privatrechtsverkehrs und als solche zurzeit von der Anwendbarkeit der Datenschutzgesetze ausgenommen (Art. 2 Abs. 2 lit. d DSG). Das Handelsregisteramt ist ein öffentliches Organ des Kantons Zürich und untersteht, mit Ausnahme der Datenbearbeitungen im Zusammenhang mit dem Handelsregister, dem kantonalen Datenschutzgesetz (§ 2 IDG). Die Aufsichtsbefugnisse der Datenschutzbeauftragten sind im Bereich des Registerrechts entsprechend eingeschränkt. Das Handelsregisteramt hat aber auch im Bereich des Handelsregisterrechts das verfassungsrechtliche Legalitätsprinzip und das Grundrecht der betroffenen Personen auf informationelle Selbstbestimmung zu achten.

Das Legalitätsprinzip bedeutet, dass öffentliche Organe nur auf einer rechtlichen Grundlage handeln dürfen. Ihr Handeln muss zudem verhältnismässig sein (Art. 5 BV). Öffentliche Organe dürfen also nur die Daten bearbeiten, die sich zur Erfüllung ihrer gesetzlichen Aufgaben eignen und dafür auch notwendig sind. Das Handelsregisteramt veröffentlichte in den vorliegenden Fällen mehr Informationen, als notwendig gewesen wären, um den Registereintrag zu belegen. Es bearbeitet dadurch mehr Personendaten, als geeignet und erforderlich sind. Diese Datenbearbeitung ist unverhältnismässig und rechtswidrig.

Das Handelsregisteramt veröffentlichte in den vorliegenden Fällen jedoch mehr Informationen, als notwendig gewesen wären, um den Registereintrag zu belegen.

Die Folgen einer rechtswidrigen Bearbeitung von Personendaten müssen korrigiert werden. Der Hinweis des Handelsregisteramts auf die Unabänderlichkeit der Belege kann sich nur auf die Teile eines Belegs beziehen, der eine Eintragung belegt. Alle anderen Teile sind vom Handelsregisterrecht nicht erfasst und sind durch das Handelsregisteramt zu schwärzen, wenn nötig auch nachträglich.

Mit Inkrafttreten des revidierten Bundesgesetzes über den Datenschutz im Herbst 2023 werden die Handelsregister nicht mehr vom Geltungsbereich des Datenschutzrechts ausgenommen sein. Die Datenschutzbeauftragte wird künftig die Aufsicht beim Handelsregisteramt ausüben. Sie wird kontrollieren, ob die Anforderungen des Datenschutzes im Bereich des Handelsregisters eingehalten werden.

Datenschutzaufsicht bei den Gerichten

Die Datenschutzbeauftragte ist zuständig für die Aufsicht über die Datenbearbeitung der öffentlichen Organe des Kantons Zürich. Der Kantonsrat und die Gerichte sind von dieser Aufsicht ausgenommen, weil sonst die Gewaltentrennung nicht eingehalten werden würde. Die Ausnahme von der Aufsicht war Thema einer Anfrage, die ein Bezirksgericht betraf.

Eine Person gelangte an die Datenschutzbeauftragte. In einem Urteil des Bezirksgerichts wurde ihr Beziehungsstatus zu einer Partei des Verfahrens erwähnt und damit der Gegenpartei und der Öffentlichkeit bekannt gegeben. Die Person war besorgt über diese Bekanntgabe ihrer Daten, die sie als unverhältnismässig betrachtete. Sie war nicht Partei im Verfahren und konnte nicht den Rechtsmittelweg beschreiten.

Die Datenschutzbeauftragte verwies die Person an die Aufsichtsinstanz des Gerichts. Jedoch war unklar, wer die Aufsicht über die Datenbearbeitung der Gerichte im Kanton Zürich ausübt. Die Weisung zum Gesetz über die Information und den Datenschutz erwähnt, dass die Gerichte selbst für die Einrichtung einer Aufsichtsinstanz verantwortlich sind. Die Datenschutzbeauftragte kontaktierte die Gerichtsleitung des Bezirksgerichts. Das Bezirksgericht klärte die Frage mit dem Obergericht. Die Verwaltungskommission des Obergerichts ist die zuständige Aufsichtsinstanz über die Gerichte im Kanton Zürich.

Schulen, Schulpflege, Elternrat und die Informationsflüsse

Schulen bearbeiten sehr viele, oft sensitive Daten von Kindern. Durch die Schulpflicht sind die meisten Einwohnerinnen und Einwohner des Kantons davon betroffen. Aus den Schülerdaten entstehen Persönlichkeitsprofile. Viele Personen und Instanzen greifen auf diese Daten zu.

Die Datenschutzbeauftragte beantwortete Anfragen zum Austausch von Informationen zwischen der Schule und der Schulpflege oder dem Elternrat.

Elternrat: Adressen der Eltern nur nach Einwilligung

Eine Schule fragte die Datenschutzbeauftragte, ob sie dem Elternrat die E-Mail-Adressen der Eltern der Schulkinder abgeben dürfe. Der Elternrat wollte Mitglieder werben und die Eltern auf Elternbildungsanlässe hinweisen. Der Elternrat ist ein selbstständig organisiertes Gremium, das die Schule aktiv unterstützt. Er ist aber nicht Teil des öffentlichen Organs Schule.

Die Schule darf Personendaten bearbeiten, wenn dies zur Erfüllung des gesetzlichen Bildungsauftrags geeignet und erforderlich ist. Die Bekanntgabe der Elternadressen an den Elternrat ist jedoch nicht erforderlich. Deshalb riet die Datenschutzbeauftragte, dass die Schule bei den Eltern eine Einwilligung zur Weitergabe der E-Mail-Adresse einholt.

Die Bekanntgabe der Elternadressen an den Elternrat ist nicht erforderlich zur Erfüllung des gesetzlichen Bildungsauftrags der Schule.

Die Bekanntgabe der Informationen an den Elternrat muss verhältnismässig sein, auch wenn die Eltern eingewilligt haben. Die verantwortliche Schule muss sich gut überlegen, welche Daten zur Kontaktaufnahme am besten geeignet sind. Nur diese Informationen dürfen an den Elternrat weitergegeben werden. Die Schule muss sich gemeinsam mit dem Elternrat überlegen, ob Handynummern, E-Mail-Adressen oder Adressdaten am geeignetsten sind.

Schulpflege: Anspruch auf Informationen nur im Einzelfall

Lehrpersonen, Schulverwaltungen und Schulleitungen meldeten sich bei der Datenschutzbeauftragten mit Fragen zu Einsichtsrechten der Schulpflege. Die Schulpflege leitet und beaufsichtigt die Schule. Sie hat im Einzelfall Anspruch auf alle Informationen, die sie zur gesetzlichen Aufgabenerfüllung benötigt, beispielsweise Informationen zu Massnahmen der Sonderschulung oder Mitarbeiterbeurteilungen. In dieser Formulierung ist der Grundsatz der Verhältnismässigkeit verankert: Mitglieder haben also nicht uneingeschränkt Zugang zu den Informationen, sondern nur im Einzelfall und nur zu den Informationen, die sie für die Erfüllung ihrer gesetzlichen Aufgabe benötigen.

Schulpflegemitglieder haben nicht uneingeschränkt Zugang zu den Informationen, sondern nur im Einzelfall.

Die gleichen Überlegungen führen auch zur Erkenntnis, dass Schulpflegemitglieder kein Anrecht auf den Schlüssel für die Zimmer der Schulverwaltung haben, wo sie Zugang zu allen Dossiers hätten, die sich dort befinden.

Der Teufel steckt im Detail

Einwohnerregister von Gemeinden enthalten viele interessante Daten. Mit einer Adressauskunft können Private Daten aus diesen Registern verlangen. Die Regeln erscheinen einfach. Sie sind für die Bevölkerung und die Gemeinden aber nicht immer klar.

Es gibt drei Arten von Auskünften: die voraussetzungslose Adressauskunft, die erweiterte Adressauskunft und die Listenauskunft. Sie sind im Gesetz über das Meldewesen und die Einwohnerregister (MERG) geregelt. Gemeinden und Privatpersonen stellen der Datenschutzbeauftragten jedes Jahr dutzende Fragen zum Thema Adressauskunft.

Unter den Anfragen verstecken sich Knacknüsse. Den Einwohnerinnen und Einwohnern stellt die Datenschutzbeauftragte auf www.datenschutz.ch *(https://www.datenschutz.ch/meine-rechte-einfordern/ihr-recht-auf-datensperre)* Vorlagen zur Verfügung, um eine Datensperre zu beantragen.

Interessensabwägungen bei Adressauskünften

Bei der voraussetzungslosen Adressauskunft gibt die Gemeinde Name, Vorname, Adresse sowie Datum von Zu- und Wegzug bekannt. Für die voraussetzungslose Adressauskunft braucht es keine Begründung der Person, die eine Auskunft will. Die Gemeinden müssen eine voraussetzungslose Adressauskunft grundsätzlich erteilen.

Eine Gemeinde fragte die Datenschutzbeauftragte, ob sie eine Adressauskunft verweigern könne, wenn ihr die Anfrage verdächtig erscheine. Die Datenschutzbeauftragte erklärte die Regeln. Auch bei der voraussetzungslosen Adressauskunft müssen die Interessen der beteiligten Personen gegeneinander abgewogen werden. Die Gemeinde kann beispielsweise die Auskunft verweigern, wenn ihr bekannt ist, dass die Person, die eine Adressauskunft will, die betroffene Person bedroht. Ein Verdacht ohne konkrete Hinweise reicht jedoch nicht aus.

Für eine erweiterte Adressauskunft muss die ersuchende Person der Gemeinde ein berechtigtes Interesse an den Daten darlegen. Die erweiterte Adressauskunft umfasst zusätzliche Informationen über Zuzugs- und Wegzugsort, Geburtsdatum, Geschlecht, Zivilstand und Heimatort. Der Auskunft darf kein überwiegendes Interesse entgegenstehen. Die Gemeinde muss diese Abwägung selbst vornehmen. Für die Adressauskunft darf die Gemeinde keine Gebühren verrechnen.

Die Adressauskunft als Namensauskunft

Eine Gemeinde wollte von der Datenschutzbeauftragten wissen, ob sie eine Adressauskunft erteilen darf, wenn die gesuchstellende Person den Namen einer Person wissen will, die an einer bestimmten Adresse wohnt. Die Gemeinde erhielt die Anfrage aufgrund eines Streits um einen Parkplatz. Das Gesetz über das Meldewesen und die Einwohnerregister sieht vor, dass die Adressauskunft auch als Namensauskunft genutzt werden kann.

Kommerzielle Interessen bei Listenauskünften

Die Listenauskunft ermöglicht eine Auskunft über eine Gruppe von Personen. Mit der Listenauskunft können Daten über mehrere Personen nach einem bestimmten

Gesichtspunkt verlangt werden, beispielsweise die Adressen aller Eltern von Kindern im Primarschulalter. Die Gemeinde darf eine Listenauskunft erteilen, wenn die Daten für ideelle Zwecke verwendet werden, beispielsweise zur Förderung der sportlichen Betätigung von Kindern. Die Person, die Auskunft verlangt, darf die Daten nicht weitergeben.

Privatpersonen fragen die Datenschutzbeauftragte oft, warum es zulässig ist, dass ihnen gemeinnützige Institutionen «Werbung» schicken. Hier erklärt sie, dass die Gemeinde Listenauskünfte für ideelle Zwecke erteilen darf. In einigen Fällen beurteilt die Datenschutzbeauftragte wie die anfragende Person die Sendung als kommerziell. Dann berät sie die betroffenen Personen über ihre Rechte.

Kein Zugang zur Listenauskunft für öffentliche Organe

Eine Gemeinde fragte die Datenschutzbeauftragte, ob sie einer Universität für die Einladung zu einer Studie Adressen ihrer Einwohnerinnen und Einwohner bekannt geben darf. Die Datenschutzbeauftragte erklärte der Gemeinde, dass die Listenauskunft nur Privaten zur Verfügung steht. Die Universität ist ein öffentliches Organ. Somit darf die Gemeinde der Universität im Rahmen der Listenauskunft keine Adressen bekannt geben. Für die Bekanntgabe bräuchte es eine andere gesetzliche Grundlage.

Die Universität ist ein öffentliches Organ. Somit darf die Gemeinde der Universität im Rahmen der Listenauskunft keine Adressen bekannt geben.

Möglichkeit der Datensperre wenig bekannt

Einwohnerinnen und Einwohner können der Gemeinde verbieten, Auskünfte zu erteilen. Das Gesetz über die Information und den Datenschutz sieht eine Datensperre vor. Wird eine Datensperre im Einwohnerregister eingerichtet, darf die Gemeinde voraussetzungslos keine Daten zu dieser Person mehr an Private bekannt geben. Die Datenschutzbeauftragte stellt auf ihrer Website einen Musterbrief für die Datensperre im Einwohnerregister zur Verfügung. Dieser Brief ist an die Einwohnerkontrolle der zuständigen Gemeinde zu schicken.

Die Gemeinde gibt Daten aus dem Einwohnerregister trotz Datensperre bekannt, wenn die Sperre die Person, die Auskunft will, an der Verfolgung eigener Rechte hindern würde.

Die Gemeinde gibt Daten aus dem Einwohnerregister trotz Datensperre bekannt, wenn die Sperre die Person, die Auskunft will, an der Verfolgung eigener Rechte hindern würde. Eine Gemeinde fragte, ob eine Datensperre durchbrochen werden darf, wenn die ehemalige Vermieterin einer neu zugezogenen Person offene Rechnungen eines alten Mietverhältnisses einfordern will. In solchen Fällen nimmt die Datenschutzbeauftragte die Interessensabwägung nicht selbst vor. Dies ist Aufgabe der Gemeinde. Sie erklärt beispielsweise, was unter «Verfolgung eigener Rechte» zur Aufhebung der Datensperre bedeutet. Die Gemeinde muss die Aufhebung der Datensperre der betroffenen Person in einer anfechtbaren Verfügung mitteilen. Sie darf die Daten bis zum Ablauf der Rechtsmittelfrist nicht bekannt geben.

Ein Datenschutzvorfall im Rampenlicht

Die Direktion der Justiz und des Innern (JI) meldete der Datenschutzbeauftragten Ende November 2020 einen Datenschutzvorfall. In den Jahren 2000 bis 2014 waren Desktop-Computer und Server der Staatsanwaltschaft Zürich nicht fachgerecht entsorgt worden. Möglicherweise habe ein Datenmissbrauch durch Drittpersonen stattgefunden.

Welche Art von Personendaten vom Vorfall betroffen waren, wurde zu diesem Zeitpunkt noch abgeklärt. Die JI hatte bereits Strafanzeige erstattet und eine Administrativuntersuchung in Auftrag gegeben, um den Vorfall abzuklären.

Die Datenschutzbeauftragte prüft bei Eingang einer Meldung im Rahmen ihrer Aufsichtsfunktion den Sachverhalt und die bereits getroffenen Massnahmen zur Wiederherstellung der Informationssicherheit und zur Verhinderung von zukünftigen Vorfällen. Sie kann zusätzliche Massnahmen anordnen und verlangen, dass die betroffenen Personen informiert werden.

Öffentliche Organe sind verpflichtet, der Datenschutzbeauftragten unbefugte Datenbearbeitungen oder den Verlust von Personendaten zu melden, wenn die Grundrechte der betroffenen Personen gefährdet sind.

Nach mehrmaligem Nachfragen erhielt die Datenschutzbeauftragte den Schlussbericht der Administrativuntersuchung sowie die Liste der Massnahmen und Zuständigkeiten Ende Mai 2021. Sie prüfte die Unterlagen und verfasste ihre Stellungnahme zum meldepflichtigen Datenschutzvorfall.

Die Datenschutzbeauftragte stellte fest, dass die JI ihre Meldepflicht erfüllt hatte. Wie die Administrativuntersuchung kam auch die Datenschutzbeauftragte zum Schluss, dass die JI teilweise ihre datenschutzrechtliche Verantwortung nicht genügend wahrgenommen hatte. Die Aufträge an externe Dienstleister waren ohne standardisierte Prozesse und Vorgaben erfolgt. Die externen Dienstleister wurden ungenügend überprüft. Sie erachtete die unsystematische Vernichtung von physischen Akten ohne Sicherstellung der Dokumentation aus datenschutzrechtlicher Sicht als bedenklich.

Der Schlussbericht der Administrativuntersuchung empfiehlt mehrere Massnahmen mit hoher Priorität. Dazu gehören der Erlass von Organisationsvorschriften, die für die ganze JI verbindlich sind, sowie die systematische Kontrolle der Einhaltung der Vorschriften und die Aktualisierung von Unterlagen zur Informationsverwaltung und Informationssicherheit, beispielsweise der Zugriffskonzepte. Zudem sollen Vorschriften für die Auswahl von externen Dienstleistern erstellt werden, um sicherzustellen, dass diese die datenschutzrechtlichen Vorgaben umsetzen. Die Datenschutzbeauftragte kam zum Schluss, dass diese Massnahmen geeignet sind, um die Risiken von Persönlichkeitsverletzungen durch den Vorfall zu mindern, die Informationssicherheit wiederherzustellen und künftige ähnliche Vorfälle zu verhindern.

Zum Zeitpunkt der Stellungnahme der Datenschutzbeauftragten war nicht bekannt, welche Personen vom Vorfall betroffen waren, was der Inhalt der Dokumente war und mit welchen Vorkehrungen die betroffenen Personen sich vor den Folgen des Vorfalls schützen könnten.

Bei einem meldepflichtigen Vorfall sieht das IDG vor, dass das öffentliche Organ die vom Vorfall betroffenen Personen über den Vorfall informiert, wenn die Umstände es erfordern oder die Datenschutzbeauftragte es verlangt. Die betroffenen Personen sollen so die Möglichkeit erhalten, sich vor den Folgen des Datenschutzvorfalls zu schützen, indem sie beispielsweise ihre Passwörter ändern. Das öffentliche Organ hat abzuwägen, ob ein überwiegendes öffentliches oder privates Interesse gegen eine Information der Betroffenen besteht. Dann kann es die Information der betroffenen Person einschränken. Die Datenschutzbeauftragte prüfte deshalb, ob sie aus datenschutzrechtlicher Perspektive verlangen soll, dass die JI die vom Vorfall betroffenen Personen über den Vorfall informiert. Sie verlangte dies nicht.

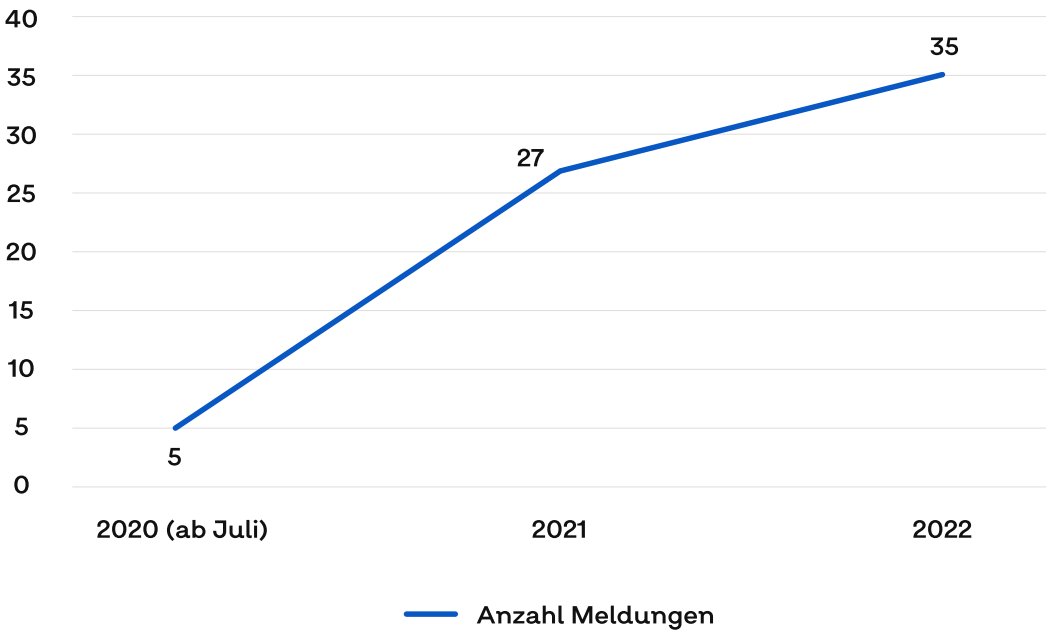
Zum Zeitpunkt der Stellungnahme der Datenschutzbeauftragten war nicht bekannt, welche Personen vom Vorfall betroffen waren, was der Inhalt der Dokumente war und mit welchen Vorkehrungen die betroffenen Personen sich vor den Folgen des Vorfalls schützen könnten. Deshalb verzichtete die Datenschutzbeauftragte darauf, die Information der betroffenen Personen zu fordern. Damit sagte sie nichts darüber aus, ob aus anderen Gründen über den Datenschutzvorfall informiert werden sollte. Die Datenschutzbeauftragte verfügt nicht über die Kompetenz, eine solche Aussage zu machen.

In ihrer Stellungnahme von Mitte September 2021 an die JI hielt die Datenschutzbeauftragte fest, dass die mit hoher Priorität festgehaltenen Massnahmen des Schlussberichts der Administrativuntersuchung umzusetzen sind. Die Umsetzung der übrigen Massnahmen wurde von der Datenschutzbeauftragten empfohlen. Sie setzte für die Umsetzung der Massnahmen mit hoher Priorität eine einjährige Frist und verlangte, dass sie über den Verlauf dokumentiert werde.

Nach Ablauf dieser Frist mahnte sie die Direktion der Justiz und des Innern und setzte eine Nachfrist bis Ende November 2022 an. Die JI äusserte Ende November 2022 gegenüber der Datenschutzbeauftragten den Wunsch, sich im Januar 2023 zum Stand der Umsetzung der Massnahmen mit der Datenschutzbeauftragten auszutauschen. Die Sache solle grundsätzlich angegangen werden.

Mehr Datenschutzvorfälle gemeldet

Die Zahl der Meldungen steigt kontinuierlich. Gingen im Jahr 2020 noch fünf Meldungen ein, waren es im Jahr 2021 bereits 27 Meldungen. Im Jahr 2022 wurden der Datenschutzbeauftragten 35 Datenschutzvorfälle gemeldet. Rund zwei Drittel der eingegangenen Meldungen stammen dabei aus dem Gesundheitsbereich.



Seit drei Jahren müssen öffentliche Organe der Datenschutzbeauftragten Datenschutzvorfälle melden. Die Statistik zeigt, dass das Bewusstsein für das Bestehen der Meldepflicht unter den öffentlichen Organen des Kantons steigt. Allerdings stammt eine Vielzahl der Meldungen von nur wenigen Institutionen. Die Datenschutzbeauftragte sieht dies als Hinweis dafür, dass in diesen Institutionen Personen mit einem besonders hohen Bewusstsein für Datenschutz und Informationssicherheit arbeiten. Damit sich dieses Bewusstsein weiterverbreitet, informiert sie an Datenschutz-Tagungen zum Thema Meldungen – so etwa am Schulthess-Forum: Datenschutz in Städten und Gemeinden.

Die Meldepflicht sensibilisiert die öffentlichen Organe und ihre Mitarbeitenden für die Schwachstellen in ihrem System. Die Datenschutzbeauftragte bekommt durch die Meldungen die Möglichkeit, die Prozesse zu kontrollieren, die offenbar Schwierigkeiten verursachen, und gleichzeitig genau da zu beraten, wo es am notwendigsten ist.

Die Datenschutzbeauftragte sieht in der Meldepflicht ein wirksames Instrument. Es vereinigt die drei gesetzlichen Aufgaben der Aufsichtsbehörden.

Die Meldepflicht sensibilisiert die öffentlichen Organe und ihre Mitarbeitenden für die Schwachstellen in ihrem System. Die Datenschutzbeauftragte bekommt durch die Meldungen die Möglichkeit, die Prozesse zu kontrollieren, die offenbar Schwierigkeiten verursachen, und gleichzeitig genau da zu beraten, wo es am notwendigsten ist.

Von fälschlich zugestellten Medikamenten und einem Hackerangriff

Die Bandbreite der Datenschutzvorfälle ist gross, welche der Datenschutzbeauftragten gemeldet wurde.

In vielen Fällen sind Einzelpersonen von der unrechtmässigen Datenbearbeitung betroffen. So wurde ein Operationsaufgebot einer falschen Empfängerin zugesandt oder ein Patient erhielt die Medikamente anderer Patientinnen und Patienten samt ihrer Personalien per Post zugestellt. In der Meldung informiert das Organ die Datenschutzbeauftragte über die bereits getroffenen Massnahmen. Die Datenschutzbeauftragte nimmt in einem standardisierten Prozess Stellung zu Vorfällen, die Einzelpersonen betreffen.

Während der Corona-Pandemie bearbeiteten öffentliche Organe grosse Mengen an besonderen Personendaten, beispielsweise im Contact Tracing. Die Medien berichteten im letzten Jahr darüber, dass Mitarbeitende des Contact Tracings auch nach ihrem Weggang noch Zugang hatten zu den über 900000 Datensätzen positiv getesteter Personen. Die Gesundheitsdirektion meldete den Vorfall der Datenschutzbeauftragten.

Bei einem Vorfall dieses Ausmasses führt die Datenschutzbeauftragte weitergehende Abklärungen durch. Sie ergaben, dass ein mangelhaftes Rechtemanagement bestand. Nach Bekanntwerden des Vorfalls wurden die nicht mehr benötigten Zugriffsberechtigungen gelöscht und die Verantwortlichkeiten wurden geklärt. Inzwischen wurde das Contact-Tracing-System abgeschaltet und alle Daten wurden entsprechend den Fristen des Covid-Gesetzes unwiderruflich gelöscht.

Im Sommer 2022 wurde die Stadt Bülach Opfer eines Ransomware-Hackerangriffs. Über mehrere Tage war die Stadtverwaltung nicht per E-Mail erreichbar. Nach erfolgter Meldung stand die Datenschutzbeauftragte mit der Stadtverwaltung im Austausch und liess sich detailliert informieren.

Die Datenschutzbeauftragte beschrieb in ihrer Stellungnahme zum Vorfall Massnahmen zur Verbesserung der Informationssicherheit. Damit soll weiteren Vorfällen vorgebeugt werden, unter anderem durch die regelmässige Sensibilisierung der Mitarbeitenden für Informationssicherheitsfragen. Für die Umsetzung der Massnahmen wird eine Frist gesetzt. Die Datenschutzbeauftragte kontrolliert die Umsetzung.

Neues Format mit neuen Möglichkeiten

Die Datenschutzbeauftragte macht den nächsten Schritt Richtung «digital only». Vor sechs Jahren hat die Behörde den Druck des Tätigkeitsberichts eingestellt. Er wurde ausschliesslich als PDF publiziert. Mit dem Tätigkeitsbericht 2022 verabschiedet sich die Datenschutzbeauftragte vom PDF, einem digitalen Überbleibsel aus der Papierwelt.

Das neue Online-Format trägt verschiedenen technischen und gesellschaftlichen Entwicklungen der letzten Jahre Rechnung. Natürlich ist diese Online-Publikation wie schon die PDF-Version barrierefrei. Neu kann sie auch auf allen mobilen Geräten mit den unterschiedlichen Displaygrössen problemlos gelesen werden. Zudem enthält der Tätigkeitsbericht jetzt audiovisuelle Inhalte.

Die Gestaltung des Tätigkeitsberichts baut auf der Bilderwelt *(https://www.datenschutz.ch/mitteilungen/2021/bilderwelt-datenschutz)* auf, die der Fotograf und Künstler Jean-Vincent Simonet für die Datenschutzbeauftragte geschaffen hat. Die Farbpalette setzt sich aus den Farbtönen eines dieser Bilder zusammen. Jedes Jahr wird ein anderes Bild im Mittelpunkt stehen.

Für die Themengebiete der Datenschutzbeauftragten eignet sich geschriebener Text auf absehbare Zeit immer noch am besten. Viele Menschen lesen längere Texte gerne in gedruckter Form. Deshalb kann der gesamte Tätigkeitsbericht zu einem PDF umformatiert und heruntergeladen werden.