dsb
datenschutzbeauftragte
des kantons zürich

Tätigkeitsbericht 2021

«Die Digitalisierung soll dem Menschen, seinen Freiheiten und dadurch der Demokratie dienen.»

Datenschutz-beauftragte des Kantons Zürich

Vorwort

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 2021 bis und mit 31. Dezember 2021 ab und ist im Internet unter www.datenschutz.ch publiziert.

Fragen zu Massnahmen während der Corona-Pandemie bestimmen auch den 27. Tätigkeitsbericht. Jedoch konnte der Fokus auf gesellschaftlich umfassendere Themen erweitert werden. Welche Bedeutung hat der Datenschutz für die Demokratie insgesamt? Wie hängt der Datenschutz mit der Demokratie zusammen? Und welche Auswirkungen hat die Digitalisierung in diesem Kontext? Die Digitalisierung soll dem Menschen, seinen Freiheiten und dadurch der Demokratie dienen. Ohne Datenschutz keine Demokratie. Es lohnt sich, sich dazu Gedanken zu machen, gerade wenn neue Lösungen ausgewählt werden.

Dr. iur. Dominika Blonski
Datenschutzbeauftragte des Kantons Zürich

Inhaltsverzeichnis

Die Demokratie muss es uns wert sein

Wo gearbeitet wird, da passieren Fehler. Oft wird vom Risikofaktor Mensch gesprochen, gerade in Zusammenhang mit der Digitalisierung. Hier zeigt sich ein grundlegend falscher Denkansatz. Der Mensch ist nicht der Risikofaktor. Er macht Fehler. Die Folgen davon können durch die Digitalisierung verstärkt werden. Man denke an die grössere Reichweite eines Datenlecks in Zeiten der Cloud im Vergleich zu damals, als die Computersysteme noch nicht vernetzt waren.

Eine Aufgabe der Informations- und Kommunikationstechnologie (IKT) sollte sein, menschliche Fehler zu verhindern oder ihre Folgen zu mindern. Nach einem Jahr Meldepflicht (Seite 12) zeigt sich, dass relativ einfache organisatorische und technische Massnahmen die meisten meldepflichtigen Datenschutzvorfälle verhindern könnten. Oft werden Mails an grosse Gruppen verschickt und die Adressen sind im Cc-Feld sichtbar. Vor allem bei häufig wiederkehrenden Versänden wäre dies vermeidbar durch den Versand über Maillisten. Wenn häufig mit mobilen Geräten und Datenträgern gearbeitet wird, wie im Homeoffice, besteht ein erhöhtes Risiko, dass ein Gerät oder ein USB-Stick irgendwo vergessen wird. Eine verschlüsselte Datenablage verhindert das Risiko einer Persönlichkeitsverletzung praktisch vollständig. Weiter ist die ständige Sensibilisierung aller Mitarbeitenden gefordert.

Digitalisierung zum Schutz der Persönlichkeitsrechte einsetzen

Privatunternehmen schieben die Verantwortung für Datenbearbeitungen und Datensicherheit über Einwilligungen weitgehend auf die Endverbraucherin oder den Endverbraucher ab. Öffentliche Organe können das nicht tun. Sie bleiben immer verantwortlich für die Daten, die ihnen anvertraut werden, ja anvertraut werden müssen. Deshalb ist eine sichere Zugangslösung bei der Online-Steuererklärung (Seite 14) unumgänglich. Das Steueramt kann die Verantwortung nicht an die Steuerpflichtigen abschieben, die hier ihr ganzes Leben offenlegen.

Oft werden die zusätzlichen Risiken der Digitalisierung einfach unterschätzt. Selbstverständlich müssen Ämter und Gemeinden über digitale Medien informieren. Wer weiss denn heute noch, wo das Amtsblatt gelesen werden könnte? Oft wird gesagt, was analog gilt, sollte auch digital gelten. Wenn es um Respekt in sozialen Medien geht, dann trifft dies sicher zu. Wenn es um die Publikation beispielsweise von Einbürgerungsdaten geht, dann eben nicht. Amtliche Publikationen von Personendaten dürfen nur zeitlich begrenzt online sein. Wenn der Zweck der Publikation erfüllt ist, dürfen sie im Internet nicht mehr gefunden werden (Seite 14).

Die Digitalisierung ist nicht einfach ein Weitermachen mit neuen Gadgets. Prozesse können und sollen neu gestaltet werden. Datenschutz muss von Anfang an mitgedacht werden. Die Schwierigkeit, Datenschutz erst dann zu integrieren, wenn sich eine Anwendung durchgesetzt hat, zeigt sich seit Jahrzehnten beim E-Mail-Verkehr (Seite 14). Bis heute konnte keine Lösung zur Verschlüsselung der Nachrichten gefunden werden, die für alle befriedigend ist. Wenn unabhängige, privat

organisierte – beispielsweise soziale – Einrichtungen mit einem Auftrag der Verwaltung untereinander kommunizieren und dabei besondere Personendaten per Mail verschicken, müssen diese Informationen verschlüsselt werden. Diese Einrichtungen arbeiten jedoch mit sehr unterschiedlichen IKT-Lösungen. Die Datenschutzbeauftragte macht auf ihrer Website www.datenschutz.ch Vorschläge, wie ein sicherer E-Mail-Verkehr unter diesen Umständen möglich ist.

Wenn aber ein Digitalisierungsprojekt am Anfang steht, kann das Auftauchen solcher Schwierigkeiten verhindert werden. Es lohnt sich, die Anliegen des Datenschutzes früh zu berücksichtigen. So verwandelt sich die Technologie von einem Risiko für die Persönlichkeitsrechte zu einem Instrument zum Schutz der Privatsphäre. Die Entwicklung der ZHservices ist ein positives Beispiel dafür (Seite 14). Die Datenschutzbeauftragte wurde früh einbezogen. Die Projektverantwortlichen kategorisierten die Daten, die über ihr zukünftiges Angebot übermittelt werden, und bestimmten die notwendigen Schutzmassnahmen für jede Kategorie. Aufgrund dieses Mappings wurden neue Technologien gesucht und gefunden, mit denen alle möglichen Services entwickelt werden können – immer mit den angemessenen Schutzmassnahmen. Ein guter Anfang ist gemacht.

Kompetenz im Umgang mit Daten

Im Rahmen verschiedener Massnahmen zur Bekämpfung der Corona-Pandemie bearbeiteten viele Personen Gesundheitsdaten, die sich bis zu diesem Zeitpunkt noch kaum mit der Sensitivität solcher Daten beschäftigt hatten (Seite 17). Durch die besondere Lage und die Bestimmungen des Epidemiengesetzes bestand zwar eine rechtliche Grundlage für weitgehende Bearbeitungen von sensitiven Personendaten. Sie lieferte aber keinen Freipass zum Austausch von Informationen über positive Testresultate oder den Impfstatus. Jede Datenbearbeitung muss trotz rechtlicher Grundlage notwendig und verhältnismässig sein. Zudem ist sie zweckgebunden. So wäre es unverhältnismässig, die Nutzerinnen und Nutzer ganzer Schulhäuser über positive Testresultate einzelner Personen zu informieren. Auch Zugriffe der Gewerbepolizei auf die Contact-Tracing-Daten eines Erotikbetriebs sind unzulässig.

Cloud Computing erfordert zunehmende Kompetenz, Daten richtig zuzuordnen (Seite 20). Für Personendaten mögen viele Plattformen noch geeignet sein, aber was passiert, wenn besondere Personendaten oder Personendaten unter besonderen Geheimnispflichten dazwischen geraten? Oder anders: Wie werden die Abläufe organisiert, damit besondere Personendaten nicht plötzlich über eine ungeeignete Cloud-Lösung bearbeitet werden? Die Tendenz bei den grossen Anbietern geht in Richtung Integration aller Arbeitsabläufe und aller Daten. Microsoft stellt demnächst Skype for Business ein. Diese (Video-)Telefonielösung konnte bisher genutzt werden, ohne dass Metadaten an den Hersteller übermittelt wurden. Beim Nachfolgeprodukt ist dies nicht mehr möglich. Bei Telefongesprächen zwischen verschiedenen Behörden sind die Metadaten kein Problem. Wenn der psychiatrische Dienst eine Klientin oder einen Klienten anruft oder die Strafverfolgungsbehörde mit einer Person telefonisch Kontakt aufnimmt, dann ist diese Tatsache schon ein besonderes Personendatum, das einen erhöhten Schutz erfordert.

In Zeiten des Fernunterrichts mussten schnell gangbare Wege gesucht werden. Hochschulen sahen sich vor der Herausforderung, Prüfungen auf Distanz durchzuführen und dabei die Prüfungsaufsicht zu gewährleisten (Seite 23). In einigen Fällen konnte auf sogenannte Open-Book-Prüfungen umgestellt werden. Wo dies nicht möglich war, mussten die Aktivitäten der Studierenden während den Prüfungen in ihrem Zuhause überwacht werden. Öffentliche Hochschulen dürfen nur die Personendaten bearbeiten, die zur Erfüllung ihrer Aufgaben notwendig sind. Jede Bearbeitung von Personendaten ist ein Eingriff in die Grundrechte der betroffenen Person, in diesem Fall der Studentin oder des Studenten. Darum muss immer die Möglichkeit gewählt werden, die den geringsten Eingriff bedeutet. Schon das Filmen der Studierenden in ihrer Privatumgebung ist ein schwerer Eingriff in das Grundrecht der informationellen Selbstbestimmung. Doch weitergehende Komplettlösungen wie Proctorio speichern nicht nur Bild und Ton aus den Wohnräumen, sondern analysieren diese Daten wie auch unter anderem die Augenbewegungen. Wie die Algorithmen funktionieren, die hier angewendet werden, ist nicht transparent.

Der Mensch ist das Mass. Er ist nicht der Risikofaktor. Die Digitalisierung soll dem Menschen, seinen Freiheiten und dadurch der Demokratie dienen. Ohne Datenschutz keine Demokratie (Seite 27). Dafür lohnt es sich, die beste Lösung zu wählen, auch wenn es nicht immer die naheliegendste ist.

Für ein zukunfts-gerichtetes neues IDG

Das Gesetz über die Information und den Datenschutz (IDG) ist ein Technikfolgenrecht. Die Digitalisierung verlangt in diesem Bereich besondere Agilität.

Im Jahr 2020 trat ein revidiertes IDG in Kraft. Darin sind die Anpassungen vorgenommen worden, die notwendig waren aufgrund der Neuerungen in der Konvention 108+ des Europarates sowie der Schengen-relevanten EU-Richtlinie 2016/680 (TB 2019, Seite 49). Im gleichen Jahr initiierte der Regierungsrat die Totalrevision des IDG.

Mit dem revidierten IDG von 2020 wurden klarere Rahmenbedingungen für die öffentlichen Organe geschaffen. Dadurch wird die Transparenz über die Datenbearbeitungen für die Bürgerinnen und Bürger sowie alle anderen Betroffenen verbessert. Öffentliche Organe sind verpflichtet, neue Datenbearbeitungen mit einer Datenschutz-Folgenabschätzung (DSFA) auf ihr Risiko für die Persönlichkeitsrechte der Betroffenen zu prüfen (TB 2020, Seite 42). Zudem haben öffentliche Organe Datenschutzverletzungen der Datenschutzbeauftragten zu melden (TB 2020, Seite 43). Gleichzeitig stärken neue Instrumente die Aufsicht durch die Datenschutzbeauftragte.

Die Totalrevision des IDG geschieht mit einem erweiterten Fokus: Das Gesetz soll an die Bedürfnisse der digitalisierten Verwaltung angepasst werden. Das Bedürfnis nach einem offeneren Datenaustausch und einem einfacheren Zugang zu Informationen soll mit den Ansprüchen der Betroffenen auf den Schutz ihrer Grundrechte in Einklang gebracht werden. Auch die Erkenntnisse aus einer mehrjährigen Evaluation des IDG (TB 2017, Seite 9) sollen berücksichtigt werden. Die Vernehmlassung ist für das Jahr 2022 vorgesehen. Die Datenschutzbeauftragte war in der Arbeitsgruppe zur Erarbeitung des neuen IDG vertreten. Sie platzierte einige grundlegende Fragen, die berücksichtigt wurden. Der Entwurf bildet insgesamt eine gute Grundlage für die Vernehmlassung.

Mit dem Konzept des heutigen IDG legte der Kanton Zürich bereits zu Beginn der 2000er-Jahre eine Grundlage für eine digitale Verwaltung. Das Gesetz regelte gleichzeitig den Zugang zu Informationen und den Schutz der Informationen. Das Öffentlichkeitsprinzip und der Datenschutz wurden als die zwei Seiten derselben Medaille gesehen. Dieses Konzept hat sich bewährt. Es regelt in einer 360°-Sicht den Umgang mit Informationen und Daten kompakt und umfassend. Der Entwurf übernimmt dieses Konzept nicht. Er trennt das Öffentlichkeitsprinzip (Informationszugang) und den Datenschutz. Dadurch verliert das IDG seine Kompaktheit. Für die öffentlichen Organe wird das Bearbeiten von Informationen und Personendaten auseinandergenommen. Personendaten sind jedoch lediglich eine Teilmenge der Informationen, für die Spezialregeln gelten. Die Verfahren, die Rechte der Betroffenen und die Aufgaben sowie Befugnisse der Aufsichtsbehörde werden ohne Notwendigkeit gespalten.

Im Zweckartikel des IDG (§ 2) wird neu die Förderung des Zugangs zu offenen Behördendaten geregelt. Mit einer zusätzlichen Erweiterung hätten auch die Rahmenbedingungen für neue Informationstechnologien wie Künstliche Intelligenz oder Blockchain geschaffen werden können.

Der Entwurf für das IDG behält die klaren Rahmenbedingungen des Öffentlichkeitsprinzips und des Datenschutzes für die Bearbeitung von Informationen inklusive Personendaten bei. Die Verfahren und Rechte der betroffenen Personen werden für den Informationszugang und den Datenschutz separat geregelt. Die öffentlichen Organen können neu Pilotversuche durchführen, in denen auch besondere Personendaten bearbeitet werden. Im Alltag wie in der IDG-Evaluation wurde die fehlende Beratung und Aufsicht für alle öffentlichen Organe und die Betroffenen im Bereich des Öffentlichkeitsprinzips kritisiert. Dieser Kritik wird mit der Schaffung der erweiterten Funktion einer oder eines Beauftragten für das Öffentlichkeitsprinzip und den Datenschutz Rechnung getragen.

Kompetent und verständlich

Zur Online-Befragung im Oktober 2021 lud die Datenschutzbeauftragte die Personen ein, die in den zwölf Monaten vor August 2021 mit ihrer Behörde in Kontakt waren. Die Befragung ist Teil der Qualitätssicherung, wie sie in der ISO-Norm 9001 vorgesehen ist. Mit der Durchführung der Befragung war das Statistische Amt des Kantons Zürich beauftragt.

Die Fachkompetenz und die Freundlichkeit der Mitarbeitenden der Datenschutzbeauftragten werden besonders gut bewertet. Die Kundinnen und Kunden beurteilten die Fähigkeit, Anliegen zu verstehen und verständlich zu beantworten, als sehr gut. Weiter zeigte sich, dass der Stellenwert des Datenschutzes am Arbeitsplatz von 88 Prozent der Befragten als hoch eingeschätzt wird. Im Vergleich zu vor vier Jahren denken deutlich mehr Befragte, dass Personendaten in ihrem Umfeld immer korrekt verwendet werden, nämlich 83 Prozent im Jahr 2021 im Vergleich zu 65 Prozent der Befragten im Jahr 2017.

Datenschutz und Informationssicherheit sind sehr spezifische Fachgebiete. Gleichzeitig betreffen die Themen Personen in den unterschiedlichsten Bereichen und Arbeitsumfeldern. Deshalb ist es besonders wichtig, dass die Informationen der Datenschutzbeauftragten adressatengerecht formuliert sind. Die Antworten der Dienstleistung der Rechtsberatung wurden von 82 Prozent der Befragten als gut verständlich beurteilt. Die Informationssicherheitsberatung kam auf einen Excellence-Wert von 84 Prozent. 69 Prozent gaben an, die Informationen auf der Website seien gut verständlich.

Allerdings kam es häufiger zu Verzögerungen bei der Beantwortung von Anfragen. Die Termintreue wurde 2021 noch von 65 Prozent als gut bezeichnet, während es 2017 noch 80 Prozent waren. Die Datenschutzbeauftragte führt dies auf die vielen sehr dringenden Geschäfte im Bereich der sich ständig ändernden Corona-Massnahmen zurück.

Wiederaufnahme der Kontrollen trotz Corona

Die Leistungsindikatoren im Konsolidierten Entwicklungs- und Finanzplan (KEF) der Datenschutzbeauftragten zeigen eine stabile Entwicklung.

Durch die andauernde Corona-Pandemie und die fortschreitende Digitalisierung bleibt der Bedarf der öffentlichen Organe an Beratung gross. Die Anzahl der Beratungen durch die Datenschutzbeauftragte hat 2021 nach einem starken Anstieg im Vorjahr nur leicht abgenommen. Neben neuen Anfragen konnten Beratungen in Digitalisierungsprojekten wieder aufgenommen werden, die aufgrund der Pandemie zurückgestellt werden mussten.

Im ersten Jahr der Pandemie verhinderten die Corona-Massnahmen die Durchführung von Besuchen vor Ort und damit die Durchführung von Kontrollen. Im zweiten Pandemiejahr wurden vermehrt Kontrollen durchgeführt. Einerseits konnten Besuche vor Ort stattfinden, andererseits waren immer mehr Organe für eine virtuelle Durchführung eingerichtet. Kontrollen verlaufen über einen längeren Zeitraum. Im KEF sind nur die abgeschlossenen Kontrollen registriert. Die zunehmende Kontrolltätigkeit wird sich in den nächsten Jahren deutlich im Indikator abzeichnen.

Die Aus- und Weiterbildungen konnten im letzten Jahr auf hohem Niveau weitergeführt werden. Die Datenschutzbeauftragte stärkt mit ihrem Engagement in diesem Bereich die Datenschutzkompetenz bei den Mitarbeitenden der öffentlichen Organe und befähigt sie dadurch, die datenschutzrechtlichen und informationssicherheitstechnischen Anforderungen der Digitalisierung zu meistern.

Bei den Vernehmlassungen, Stellungnahmen und Mitberichten ist ein Zuwachs zu verzeichnen. Hier zeigt sich, dass die Fragen des Datenschutzes durch die fortschreitende Digitalisierung in immer mehr Rechtssetzungsprojekten eine wichtige Rolle einnehmen. In diesen Fällen wird die Expertise der Datenschutzbeauftragten eingeholt.

		KEF	2020	2021
Beratungen	Der Leistungsindikator im KEF misst die Anzahl der Beratungen von öffentlichen Organen und Privatpersonen in Fragen des Datenschutzes und der Informationssicherheit.	650	856	753
Kontrollen	Der Leistungsindikator im KEF misst die Anzahl der Kontrollen (Datenschutzreviews) der Anwendung der rechtlichen, technischen und organisatorischen Vorschriften in öffentlichen Organen.	60	10	22
Aus- und Weiterbildungen	Der Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote für öffentliche Organe (Seminare, Kurse, Workshops und Referate).	20	27	29
Vernehmlassungen	Der Leistungsindikator im KEF gibt Auskunft über die Anzahl der Vernehmlassungsantworten, Stellungnahmen und Mitberichte.	18	13	27

Datenschutzbeauftragte des Kantons Zürich

Die Datenschutzbeauftragte (DSB) beaufsichtigt als unabhängige Aufsichtsbehörde die Datenbearbeitungen der kantonalen Verwaltung, der Gemeinden und der übrigen Behörden und öffentlichen Einrichtungen im Kanton, um die Privatsphäre der Einwohnerinnen und Einwohner sicherzustellen.

Sie berät die öffentlichen Organe, beurteilt datenschutzrelevante Vorhaben (Vorabkontrollen) und nimmt Stellung zu Erlassen. Sie bietet Aus- und Weiterbildungen in den Bereichen Datenschutz und Informationssicherheit an.

Bei öffentlichen Organen überprüft sie mit Kontrollen (Datenschutzreviews), ob die Anforderungen des Datenschutzes in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht eingehalten sind. Öffentliche Organe sind verpflichtet, Datenschutzvorfälle zu melden. Die Datenschutzbeauftragte kann die Umsetzung von Massnahmen verfügen.

Die Datenschutzbeauftragte berät Privatpersonen über ihre datenschutzrechtlichen Ansprüche und vermittelt in Konfliktfällen zwischen Privatpersonen und öffentlichen Organen. Sie informiert die Öffentlichkeit über die Anliegen des Datenschutzes und der Informationssicherheit.

Der Alltag in der Informations-sicherheit

Seit Inkrafttreten des revidierten Gesetzes über die Information und den Datenschutz (IDG) sind Datenschutzvorfälle der Datenschutzbeauftragten zu melden. Die Meldungen zeigen die prekären Bereiche der Informationssicherheit im Alltag der Mitarbeitenden öffentlicher Organe. Sie reichen vom Versand von vertraulichen E-Mails an falsche Adressen bis zur Attacke mit einem Verschlüsselungstrojaner.

Die Datenschutzvorfälle werden über ein Formular gemeldet, das auf der Website www.datenschutz.ch verlinkt ist. So erhält die Datenschutzbeauftragte alle benötigten Informationen und kann die Relevanz des Vorfalls schnell beurteilen.

Verschlüsselungstrojaner im Spital
Im Jahr 2020 erfuhr die Datenschutzbeauftragte von einem Vorfall in einem Spital. Ein Teil der zentralen Datenablage war verschlüsselt worden. Der Verschlüsselungstrojaner war über einen E-Mail-Anhang mit einem schädlichen Makro eingedrungen. Nachforschungen ergaben, dass keine Daten entwendet worden waren. Mit dem Backup-System konnten alle Daten innerhalb von sechs Tagen wiederhergestellt werden.

Verlust von Personendaten
Ein Spital speichert Behandlungsdaten von Operationen auf mobilen Datenträgern, die an andere Teams weitergegeben werden. Einer dieser Datenträger befand sich nicht mehr am vorgesehenen Platz und konnte nicht mehr gefunden werden.

Im Rahmen seiner Arbeit speicherte ein Mitglied einer ausserparlamentarischen Kommission sensitive Informationen über Projekte eines öffentlichen Organs auf seinem Geschäfts-Notebook. Die Person löschte die Daten später. Der Arbeitgeber stellte die Daten auf dem Notebook durch das Aufspielen eines Backups wieder her und bekam so Zugang zu den sensitiven Personendaten.

Ähnliche Auswirkungen haben Vorfälle, wie der Diebstahl eines Notebooks mit Patientendaten aus der Psychiatrie oder ein liegengelassenes Notebook im Zug.

Versand von E-Mails mit sichtbarem Adressverteiler
E-Mails sind schnell versendet. Schnell sind die Mailadressen in das Adress- oder ins Cc-Feld eingegeben, ein Betreff und ein Text hinzugefügt und mit einem Klick auf «Senden» ist das Unglück geschehen. Beim Ablegen der Nachricht oder nach einer Rückmeldung einer Person, die das E-Mail erhalten hat, fällt dann auf, dass die Mailadressen aller Empfängerinnen und Empfänger sichtbar sind.

Die Datenschutzbeauftragte bekam im Jahr 2021 mehrere solche Vorfälle gemeldet. Die Inhalte der versendeten Mails liessen Schlüsse zu auf den gesundheitlichen Zustand oder die wirtschaftliche Situation der Empfängerinnen und Empfänger.

Ausgenutzte Sicherheitslücke
Im März 2021 wurde eine Sicherheitslücke bei Microsoft Exchange Server bekannt. Eine Gemeinde schloss die Schwachstelle mit einem Sicherheitsupdate des Herstellers. Sie stellte fest, dass die Sicherheitslücke ausgenutzt worden war. Untersuchungen auf der Firewall zeigten jedoch keinen signifikanten Datentransfer für die Zeit zwischen dem Bekanntwerden der Sicherheitslücke bis zum Aufspielen des Sicherheitsupdates.

Geschützte Personendaten ungeschützt auf Website
Ein öffentliches Organ stellt den Gemeinden in einem passwortgeschützten Bereich seiner Website Listen von registrierten Personen zur Verfügung. Ein Mitarbeiter stellte fest, dass die Listen über eine externe Suchmaschine für alle sichtbar waren und meldete den Vorfall an die Datenschutzbeauftragte. Gleichzeitig wurde die für die Website zuständige Stelle informiert, die den Konfigurationsfehler sofort behob.

Bessere Informationssicherheit durch Meldepflicht
Die Meldungen zeigen die alltäglichen Herausforderungen der öffentlichen Organe im Bereich der Informationssicherheit. Im direkten Austausch mit den betroffenen Institutionen kann die Datenschutzbeauftragte wirksame und praxisnahe Präventionsmassnahmen entwickeln. Diese werden in Merkblättern und Sensibilisierungsaktivitäten integriert.

Die Erfahrungen des ersten Jahres der Meldepflicht zeigen, dass den Vorfällen vordergründig oft Fehler der Mitarbeitenden zugrunde liegen. Diese können jedoch verhindert oder ihre Folgen gemindert werden, indem grundlegende technische und organisatorische Massnahmen umgesetzt werden. Mobile Datenträger müssen beispielsweise immer verschlüsselt sein. Beim Einsatz von privaten Geräten sind die Mitarbeitenden regelmässig auf die minimalen Sicherheitsanforderungen aufmerksam zu machen. Dazu gehören beispielsweise eine Bildschirmsperre, die nach einer kurzen Zeitspanne automatisch aktiviert wird, oder die routinemässige Aktualisierung der Betriebssysteme und der Software.

Komfort und Sicherheit dank Digitalisierung

Die Dienstleistungen des Kantons, der Gemeinden, der Schulen oder Spitäler sollen komfortabler werden für die Einwohnerinnen und Einwohner. Dazu bietet die Digitalisierung viele Möglichkeiten. Ebenso viele Möglichkeiten bestehen, damit die Technologie von einem Risiko für die Persönlichkeitsrechte zu einem Instrument zum Schutz der Privatsphäre wird.

Online-Steuererklärung sicher machen
Die Steuererklärung kann im Kanton Zürich seit 2020 online ausgefüllt und eingereicht werden. Die Datenschutzbeauftragte hatte das Steueramt in Bezug auf einzelne Fragen beraten. Sie äusserte sich kritisch, dass Steuerpflichtige nur durch die Eingabe der AHV-Nummer und eines Passworts auf Steuerdaten aus dem Vorjahr zugreifen können. Bei Online-Angeboten im Finanzbereich ist der Zugriff auf diese Personendaten über eine Zwei-Faktor-Authentifizierung Standard. Nach heutigem Stand der Technik stellt eine Zwei-Faktor-Authentifizierung durch zwei unterschiedliche und voneinander unabhängige Komponenten sicher, dass sich ausschliesslich die berechtigte Person anmelden kann. Sie schützt einerseits die Daten der Betroffenen zuverlässig, andererseits sichert sie deren Vertrauen in das Angebot der Institution. Das Steueramt hat für die Steuererklärung 2021 als Übergangslösung einen SMS-Code als zusätzlichen Faktor für die Anmeldung und das Abrufen von Vorjahres- und aktuellen Daten eingeführt. Auch die neue Lösung entspricht nicht dem State of the Art im Umgang mit Finanzdaten. Sie ist aber eine starke Verbesserung gegenüber der Zugangslösung im Jahr 2020. Sie berücksichtigt die Herausforderungen, die durch die Aufgabenverteilung zwischen dem kantonalen Steueramt und den kommunalen Steuerämtern entstehen. Mittelfristig sieht die Datenschutzbeauftragte eine vollständig umgesetzte Zwei-Faktor-Authentifizierung als unumgänglich. Besonders bei Plattformen mit besonderen Personendaten oder solchen, die einer besonderen Geheimnispflicht unterstehen, wie Gesundheits- oder Steuerdaten, ist dies als implementierte Grundfunktion erforderlich. Diese muss mit der Einführung des Zürikontos angeboten werden können. Zudem hat das Steueramt weitere technische Mängel behoben.

Schutz von Einbürgerungsdaten im Internet
Eine Bürgerin machte die Datenschutzbeauftragte darauf aufmerksam, dass auf der Website einer Gemeinde die Daten von Einbürgerungswilligen auch nach mehr als einem Jahr noch abrufbar waren. Sie hatte zuvor die Gemeinde aufgefordert, diese Informationen von der Website zu entfernen, da der Zweck der Veröffentlichung nach der Einbürgerung erfüllt sei. Die Bürgerin verwies die Gemeinde auf die Publikation der Datenschutzbeauftragten Veröffentlichung von Einbürgerungsdaten. Die Datenschutzbeauftragte wies die Gemeinde darauf hin, dass Personendaten im Internet eines höheren Schutzniveaus bedürfen. Bei einer Veröffentlichung im Internet bestehen höhere Risiken einer Persönlichkeitsverletzung als bei der Veröffentlichung in einer gedruckten Zeitung. Die Daten sind einem unbegrenzten Personenkreis zugänglich, über die Suchmaschine einfach auffindbar und können nur schwer gelöscht werden. Diese Risiken sind durch technische Massnahmen zu verringern. Die Publikationsdauer ist einzuschränken. Die Indexierung durch Suchmaschinen ist zu verhindern, indem beispielsweise der Meta-

Tag «noindex» in den HTML-Code der Seite aufgenommen wird.

Go-live in der Gemeinde
Die Datenschutzbeauftragte beriet eine Gemeinde bei der Erarbeitung eines neuen Webauftrittes. Sie verwies dabei auf ihre Publikationen, beispielsweise die Merkblätter Sichere Website und Dienste Dritter auf Websites sowie auf den Webartikel Datenschutzerklärung auf Websites öffentlicher Organe. Sie enthalten detaillierte Informationen und Checklisten. Beim Aufrufen einer Website geben die Nutzerinnen und Nutzer ihre IP-Adresse bekannt. Dieses Personendatum darf bearbeitet werden, weil sich der Betrieb einer Website aus dem Informationsauftrag ergibt. In den meisten Fällen wird die Website über einen externen Dienstleister angeboten. Die Verantwortung für die datenschutzkonforme Bearbeitung der Personendaten liegt in jedem Fall beim öffentlichen Organ. Dies gilt auch für Dienste durch Dritte wie eine externe Suchfunktion oder einen Dienst zur Erstellung von Webstatistiken. Deshalb ist ein schriftlicher Vertrag zwischen dem öffentlichen Organ und dem Dienstleister notwendig. Öffentliche Organe dürfen Personendaten nur bearbeiten, wenn dafür eine rechtliche Grundlage besteht. Deshalb ist eine Datenschutzerklärung nicht notwendig.

Digitales Arbeiten im Schulzimmer
Schulen, Lehrpersonen sowie Schülerinnen, Schüler und ihre Eltern stellten der Datenschutzbeauftragten im letzten Jahr vor allem Fragen zu Bring Your Own Device (BYOD), zur Überwachung privater Notebooks, aber auch zur Nutzung von umfassenden Datenbearbeitungen mit Produkten wie Klapp oder Classtime.

Der Einsatz von privaten Geräten ist in einer BYOD-Weisung festzuhalten. Schulen müssen definieren, welche Mitarbeitenden der Schule unter welchen Umständen Zugriff auf das private Gerät haben. Dabei ist zu berücksichtigen, dass bei einer Situation der Bedrohung der lokalen Sicherheit vielleicht Analyse- und Auswertungsdaten abgefragt werden müssen. Die Schülerinnen und Schüler sind zu verpflichten, die grundlegenden Sicherheitsmassnahmen umzusetzen. So muss das Gerät mit einem Passwort vor unberechtigten Zugriffen geschützt sein und die Bildschirmsperre muss nach spätestens 15 Minuten automatisch aktiviert werden. Das Betriebssystem und die Software sind auf dem aktuellsten Stand zu halten. Die lokale Firewall und der Malwareschutz sind zu aktivieren. Die Festplatte ist zu verschlüsseln und Schul- und Schülerdaten sind getrennt von den privaten Daten zu speichern. Wichtig ist ebenfalls eine klare Regelung, welche Daten auf dem privaten Gerät überhaupt gespeichert werden dürfen und wie die Datensicherung erfolgen muss. Wenn über das Internet auf Ressourcen der Schule zugegriffen wird, muss dafür eine Zwei-Faktor-Authentifizierung bestehen, sowohl beim Zugriff auf den Schulserver wie auf Cloud-Dienste. Die Datenschutzbeauftragte hat zu diesem Thema den Leitfaden Einsatz mobiler Geräte in der Verwaltung veröffentlicht.

Für den Einsatz von Online-Tools im Schulunterricht gilt, dass nicht alle Produkte für alle Arten von Daten geeignet sind. So kann Klapp beispielsweise in der Schule genutzt werden. Da aber eine Verschlüsselung der Datenbank fehlt, dürfen besondere Personendaten nicht bearbeitet werden. Die datenschutzkonforme Nutzung von Classtime ist unter dem Rahmenvertrag von educa möglich.

Sorge tragen für Personendaten
Besondere Personendaten müssen beim E-Mail-Verkehr verschlüsselt werden. Kompliziert wird es, wenn die Behörden untereinander verschiedenste Verschlüsselungstechniken verwenden und die Dienstleister der einzelnen Behörden unterschiedlicher Meinung sind. Eine kantonale Aufsichtsstelle unterbreitete der Datenschutzbeauftragten diese Problematik, die den Mailverkehr unter den Institutionen behinderte, die ihr unterstellt sind. Die Datenschutzbeauftragte zeigt in solchen Fällen auf, was der Stand der Technik ist und erklärt den Sachverhalt, damit dieser auch ohne tiefe Fachkenntnisse verständlich ist. Ein Überblick der Verschlüsselungsmöglichkeiten ist im Merkblatt Softwarelösungen für IT-Verantwortliche zu finden.

Über die ZHservices stellt der Kanton den Einwohnerinnen und Einwohnern sowie Unternehmen, aber auch öffentlichen Organen schon jetzt viele Dienste zur Verfügung, zum Beispiel die Online-Steuererklärung. Die Dienste sollen im Rahmen des Impulsprogramms Digitalisierung erneuert und erweitert werden. Die Datenschutzbeauftragte wurde früh in das Projekt einbezogen, wodurch die Datenschutzthemen von Beginn an berücksichtigt werden konnten. Bereits in den ersten technischen Informationen, die der Datenschutzbeauftragten zur Verfügung gestellt wurden, waren wesentliche Punkte integriert, wie Datensparsamkeit, personengebundene Berechtigungen, mehrschichtiges Verschlüsselungssystem, klare Trennung der Aufgaben und Verantwortlichkeiten. Die modulare und offene Architektur des Systems erlaubt es, in Zukunft neue Technologien zu integrieren. Dieser Aspekt wird an Bedeutung gewinnen. Die Technologie entwickelt sich rasant und neue Sicherheitstechniken müssen schnell angewendet werden können. Schon während der Projektphase konnten so neue Verschlüsse-

lungstechnologien integriert werden. Durch die modulare Bauweise können Sicherheitsmassnahmen eingebunden werden, die den optimalen Schutz für die verschiedenen Datenkategorien gewährleisten – von Personendaten über besondere Personendaten bis hin zu Personendaten unter Geheimnispflichten. Damit die angemessenen Sicherheitsmassnahmen eingesetzt und die Daten der Bevölkerung optimal geschützt werden können, müssen zuerst die Daten identifiziert und kategorisiert werden, die über ZHservices bearbeitet werden sollen.

Blockchain, Künstliche Intelligenz und die kantonale Verwaltung
Die Datenschutzbeauftragte arbeitete am Leitfaden Blockchain in der kantonalen Verwaltung mit. Dies, nachdem sie bei der Erarbeitung der Blockchain-Studie beteiligt war. Im Rahmen von kantonalen und interkantonalen Workshops wurden Anwendungsfälle besprochen. Daraus wurde eine Anleitung erstellt, mit der überprüft werden kann, ob der Einsatz von Blockchain-Technologie geeignet ist. Die Datenschutzbeauftragte erläuterte, dass der Begriff der Blockchain-Technologie zu regeln ist und verbindliche Vorgaben für ihren Einsatz festgelegt werden müssen. Sie wies darauf hin, dass Fragen zur Löschung und zur Korrektur von Angaben in der Blockchain ungelöst sind.

In Workshops und mit Interviews beteiligte sich die Datenschutzbeauftragte an einer Studie des Kantons zu möglichen Einsatzbereichen der Künstlichen Intelligenz in der öffentlichen Verwaltung. Die Studie lief als Vorprojekt im Projekt IP 6.4 des Impulsprogramms Digitalisierung. Sie sollte aufzeigen, wo das Potenzial von Künstlicher Intelligenz liegt und welche rechtlichen und ethischen Rahmenbedingungen beim Einsatz in der kantonalen Verwaltung zu berücksichtigen sind. Die Datenschutzbeauftragte wies darauf hin, dass zuerst festgelegt werden soll, wofür die Künstliche Intelligenz eingesetzt wird. Danach muss abgeklärt werden, ob sie für diesen Einsatz überhaupt geeignet ist. Für den Einsatz Künstlicher Intelligenz muss erst eine Rechtsgrundlage geschaffen werden. Bei jedem Projekt, in dem Künstliche Intelligenz eingesetzt werden soll, ist nach einer Datenschutz-Folgenabschätzung auch eine Vorabkontrolle durch die Datenschutzbeauftragte durchzuführen, da es sich um eine neue Technologie handelt. Die Prozesse der Künstlichen Intelligenz verschleiern die Transparenz der Datenbearbeitungen für die Betroffenen, was das Vertrauen in die öffentlichen Organe gefährdet. Dem muss entgegengewirkt werden, indem die Verfahren, die Entscheidungsabläufe und die Möglichkeiten, sich dagegen zu wehren, besonders gut erklärt werden. Diese Anforderungen müssen in die Gesetzgebung einfliessen.

Rechtsverbindlicher Behördenverkehr mit DigiLex
Mit dem Projekt DigiLex sollen die rechtlichen Grundlagen für einen durchgehenden rechtsverbindlichen elektronischen Behördenverkehr geschaffen werden. Die Datenschutzbeauftragte begleitete das Projekt. Sie wies darauf hin, dass eine Regelung auf Gesetzesstufe wichtig ist. Sie befürwortet, dass die Bestimmungen auf dieser Stufe knapp und technologieneutral gehalten werden. Dadurch können die Anforderungen in der Verordnung zum Gesetz konkretisiert und schnell an die technologischen Entwicklungen angepasst werden. Die Datenschutzbeauftragte begrüsste, dass die Erläuterungen wichtige Aussagen zum Inhalt der Verordnung enthalten. Bestimmungen zur Informationssicherheit sollen mehrheitlich in der Verordnung festgehalten werden. Für die Datenschutzbeauftragte steht die Sicherstellung eines angemessenen Informationssicherheitsniveaus im Zentrum, wie sie in ihrer Stellungnahme zur geplanten Anpassung des Verwaltungsrechtspflegegesetzes (VRG) festhielt.

Neue Grundlage für den E-Voting-Versuchsbetrieb
Die Datenschutzbeauftragte nahm Stellung zur Teilrevision der Verordnung über die politischen Rechte (VPR) und der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS). Sie sollen die neue Grundlage für den E-Voting-Versuchsbetrieb bilden. Neu sollen nur vollständig verifizierbare E-Voting-Systeme zum Einsatz kommen. Die Einhaltung der Sicherheitsanforderungen soll von unabhängigen Expertinnen und Experten im Auftrag des Bundes überprüft werden. Ihre Erkenntnisse sollen in einen kontinuierlichen Verbesserungsprozess einfliessen. Der Bund definiert den rechtlichen Rahmen und bleibt Bewilligungsbehörde. Die Kantone entscheiden, ob und mit welchem System sie ihren Stimmberechtigten E-Voting anbieten wollen. Die Datenschutzbeauftragte begrüsst den Ansatz, die Informationssicherheit zu stärken, die unabhängige Überprüfung und erweiterte Transparenzvorschriften einzuführen sowie die Öffentlichkeit und die Wissenschaft einzubeziehen. Der Open-Source-Ansatz ist eine gute Möglichkeit, Transparenz und Vertrauen in den Einsatz von E-Voting-Systemen aufzubauen, da Sicherheitslücken durch unabhängige Dritte entdeckt und die Sicherheit verbessert werden können. Die Datenschutzbeauftragte wies darauf hin, dass die technischen Möglichkeiten, ein E-Voting-System zu missbrauchen, nicht abschliessend eingeschätzt und deshalb nicht beherrscht werden können. Die technische Weiterentwicklung sei zudem nicht vorhersehbar. Die vorgeschlagene Neuausrichtung könne zu einer momentanen Verbesserung der Informationssicherheit führen. Die Umsetzung der Vorgaben sei jedoch fraglich. Wenn jeder Kanton sein eigenes System entwickeln lasse, müssten über 20 Systeme überprüft werden.

Gesundheitsdaten für alle überall

Gesundheitsdaten sind besondere Personendaten. Massnahmen zur Bekämpfung der Corona-Pandemie führten zu einer grossen Anzahl von Bearbeitungen von Gesundheitsdaten durch sehr viele Organisationen und Personen. Darunter waren solche, die sich bis zu diesem Zeitpunkt noch nicht mit der Sensitivität solcher Daten beschäftigt hatten.

Vacme als Impfdaten-Taschenmesser
Die Gesundheitsdirektion fasste den Entscheid, sämtliche Impfungen im Kanton Zürich in einer zentralen Impfdatenbank zu dokumentieren. Über die Plattform Vacme registriert sich die Person, die sich impfen lassen möchte. Die Plattform erfüllt dabei verschiedene Zwecke. Sie weist Impftermine zu, rechnet Kosten zwischen Krankenkassen und Kanton ab, bearbeitet Daten für die Ausstellung von Impfzertifikaten und liefert ein Reporting an den Bund gemäss der Epidemiengesetzgebung.

Diese Fülle an Datenbearbeitungen betrifft die Mehrheit der Bevölkerung im Kanton Zürich. Der grosse Umfang von Bearbeitungen von Gesundheitsdaten führt zu besonderen Datenschutzrisiken. Solche Projekte sind der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Von einer formellen Vorabkontrolle kann abgesehen werden, wenn die Datenschutzbeauftragte bereits in einem frühen Stadium des Projektes mitwirkt (§ 10 Abs. 2 IDG).

Die Gesundheitsdirektion bat die Datenschutzbeauftragte Ende 2020 um Beratung zu verschiedenen datenschutzrechtlichen Fragen im Zusammenhang mit dem Impfprogramm. Mit Rücksicht auf die besondere Dringlichkeit der Situation bot die Datenschutzbeauftragte der Gesundheitsdirektion eine begleitende Beratung des Projekts an. Eine formelle Vorabkontrolle wurde nicht durchgeführt.

Die Datenschutzbeauftragte überprüfte das Informationssicherheits- und Datenschutzkonzept (ISDS) von Vacme und beurteilte die vertraglichen Grundlagen zwischen der Gesundheitsdirektion und der externen Betreiberin der Impfplattform. Beim ISDS wurde vor allem auch auf die Sicherheit der Speichermedien geachtet und ihre Verschlüsselung verlangt. Zudem wies die Datenschutzbeauftragte darauf hin, dass ein Archivierungs- und Löschungskonzept erstellt werden müsse. Auch für die Logdaten seien die Zugriffsberechtigungen und die Löschung der Daten zu regeln. Die Gesundheitsdirektion übernahm die Hinweise. Die Datenschutzbeauftragte beriet die Gesundheitsdirektion zum Datenabgleich von Impfdaten zwischen Vacme und Vorgängersystemen.

Öffentliche Organe müssen zwar keine Datenschutzerklärungen veröffentlichen, da für ihre Datenbearbeitungen immer eine rechtliche Grundlage bestehen muss. Bei einem Projekt dieses Ausmasses in einem aufgeladenen gesellschaftlichen Umfeld mit einer verunsicherten Bevölkerung kommt der transparenten Information eine besondere Rolle zu. Die Datenschutzbeauftragte erhielt mehrere Anfragen von Privatpersonen zur Datenschutzerklärung, den Nutzungsbedingungen und zur Einverständniserklärung, die bei der Registration in Vacme akzeptiert werden mussten. Sie informierte etwa, dass ein Haftungsausschluss in den Nutzungsbedingungen zumindest datenschutzrechtlich keine Bedeutung hat. Die gesetzlichen Anforderungen bleiben bestehen.

Die Impfthematik führte zu Fragen aus ganz unterschiedlichen Bereichen. Die Datenschutzbeauftragte beriet beispielsweise ein Alters- und Pflegeheim zu den Zugriffsberechtigungen auf die Listen der geimpften Personen des Heims. Im Herbst 2021 wurde die Auffrischimpfung ausgerollt. Viele Impfwillige hatten ihre Vacme-Zugangsdaten vergessen. Die Betreiberin der Impfhotline wollte den hilfesuchenden Personen nützliche Hinweise geben. Dafür benötigten ihre Mitarbeitenden erweiterte Zugriffsberechtigungen innerhalb von Vacme. Die Datenschutzbeauftragte formulierte die Rahmenbedingungen, unter denen die Zugriffsmöglichkeiten gelockert werden konnten.

Corona-Tests überall – neue Probleme für die Schulen

Auf die Fragen zum Contact Tracing im Jahr 2020 folgten 2021 erst solche zur Impfkampagne und kurz darauf zum Testprogramm. Teil der Teststrategie des Bundes bildeten Pooltests und das repetitive Testen in Unternehmen und Schulen. Für die Umsetzung waren die Kantone zuständig. Die Gesundheitsdirektion setzte für die Durchführung der repetitiven Reihentests eine Plattform einer externen Betreiberin ein. Sie bearbeitet die Daten der Getesteten im Auftrag der Gesundheitsdirektion. Diese Daten geben Aufschluss über den Gesundheitszustand der Personen und sind somit sensitive Personendaten. Die Datenschutzbeauftragte prüfte die vertraglichen Grundlagen der Betreiberin datenschutzrechtlich mit besonderer Dringlichkeit.

Für die Schulen stellten sich im Rahmen der Testdurchführung viele herausfordernde Fragen. Wem dürfen welche Ergebnisse mitgeteilt werden? Müssen verschiedene zusammengehörende Schulhäuser über einen positiv getesteten Pool informiert werden? Wer muss über einen positiven Einzeltest informiert werden? Darf ein an den Covid-19-Reihentests beteiligtes Labor die Ergebnisse der Schule direkt melden? Sind die Eltern verpflichtet, die Ergebnisse zu melden? Falls ja, wem?

Zu derartigen Fragen hat die Datenschutzbeauftragte sowohl Eltern als auch Schulen beraten. Sie stand auch im Austausch mit dem Volksschulamt. Die Informationen zu positiven Tests mussten schnell zu den richtigen Adressatinnen und Adressaten gelangen. Andererseits war darauf zu achten, dass der Schutz der betroffenen Personen gewährleistet war. Informationen über einen positiv getesteten Pool waren zudem anders zu behandeln als das positive Einzelergebnis einer Schülerin oder eines Schülers.

Eine Schule mit mehreren Einheiten stellte die Frage, ob Eltern klassen- oder schulhausübergreifend über einen positiv getesteten Pool oder sogar über Einzelergebnisse in einer anderen Klasse informiert werden können. Die Datenschutzbeauftragte erklärte, dass positive Testresultate besondere Personendaten seien. Die vorgesehene breite Information hätte keinen Mehrwert zur Pandemiebekämpfung bedeutet. Sie war deshalb weder verhältnismässig noch erforderlich und darum nicht zulässig.

In einer Gemeinde wurde eine Mitarbeiterin eines Jugendtreffs positiv auf Corona getestet. Die betroffene Mitarbeiterin und der Jugendtreff informierten den Kantonsärztlichen Dienst, die betroffenen Kinder und ihre Eltern. Die Schule und die Gemeinde verschickten zusätzlich einen Elternbrief. Aus den detaillierten Informationen des Briefs konnte die infizierte Person eindeutig identifiziert werden. Für eine erkrankte Person ist es ein einschneidender Eingriff in ihre Persönlichkeitsrechte, wenn ihre Infektion bekannt gegeben wird. Deshalb ist der Umfang des Personenkreises so weit wie möglich zu begrenzen. Mit den Vorkehrungen des Jugendtreffs waren die gesetzlichen Vorschriften und der Zweck der Pandemieeindämmung erfüllt. Die weiteren Informationstätigkeiten waren nicht verhältnismässig.

Die Teilnahme an regelmässigen Reihentests führte zu Erleichterungen der Quarantänebestimmungen. Erleichterungen waren auch möglich, wenn ein Covid-Zertifikat vorgelegt wurde. Dies warf die Frage auf, in welcher Form die Schulen Zertifikate überprüfen, einfordern, abspeichern oder Lehrpersonen zugänglich machen durften. Die Datenschutzbeauftragte beriet die Bildungseinrichtungen. Zertifikate von Schülerinnen und Schülern dürfen nicht aufbewahrt werden. Sie müssen jeweils geprüft und in einer Liste vermerkt werden.

Kontaktdaten in Erotikbetrieben
Die Corona-Massnahmen führten im Jahr 2021 auch neben den Impf- und Testprogrammen zu sehr weitgehenden Datenerhebungen. Im Rahmen des Contact Tracings mussten auch Erotikbetriebe die Kontaktdaten ihrer Kunden erheben und aufbewahren. Ein Betrieb gelangte an die Datenschutzbeauftragte, da die Sorge bestand, dass bei gewerbepolizeilichen Kontrollen in unzulässiger Weise auf die Kontaktdaten der Kunden Zugriff genommen werden könnte. Die Datenschutzbeauftragte ging spezifisch auf den Zweckbindungsgrundsatz ein. Kontaktdaten von Gästen werden zum Zweck der Pandemiebekämpfung erhoben und dürfen nur für diesen Zweck eingesehen werden. Für andere Zwecke, etwa für gewerbepolizeiliche Kontrollen, stehen diese Daten nicht zur Verfügung. Die Einhaltung der Corona-Massnahmen darf kontrolliert werden. Dafür können Stichproben der Kontaktdaten auf ihre Korrektheit überprüft werden.

Mitwirkung von Ärztinnen und Ärzten in KESB-Verfahren
In der Gesetzgebung zum Kindes- und Erwachsenenschutzrecht finden sich Mitwirkungspflichten und Mitwirkungsrechte für Ärztinnen und Ärzte. Sie unterstehen jedoch dem Berufsgeheimnis nach Art. 321 Strafgesetzbuch. Ein Spital fragte die Datenschutzbeauftragte, unter welchen Voraussetzungen ihre Ärztinnen und Ärzte Gesuche um Datenbekanntgabe durch KESB-Behörden bearbeiten dürfen. Bei erwachsenen Patientinnen und Patienten müssen diese einer Datenbekanntgabe zustimmen oder es muss eine Entbindung vom Berufsgeheimnis vorliegen. Bei Kindern sind Ärztinnen und Ärzte auch ohne Entbindung zur Mitwirkung berechtigt.

Meldepflicht bei Krebserkrankungen
Im Krebsregister werden Personendaten und hauptsächlich besondere Personendaten zusammengeführt, damit sie in der Epidemiologie und der Forschung genutzt werden können. Für Datenbearbeitungen zu Forschungszwecken ist grundsätzlich eine ausdrückliche Einwilligung der betroffenen Person nach vollständiger Aufklärung nötig. Für das Krebsregister ist spezialgesetzlich eine Ausnahme von diesem Grundsatz vorgesehen. Die betroffenen Personen haben nur ein Widerspruchsrecht (Art. 6 des Bundesgesetzes über das Krebsregister (KRG, SR 818.33)). Darin liegt eine Schwächung des Selbstbestimmungsrechts der betroffenen Personen. Sie ist vor dem Hintergrund der mit dem Krebsregister verfolgten Ziele hinzunehmen. Allerdings muss sichergestellt werden, dass jede betroffene Person über ihr Widerspruchsrecht informiert ist. Dies wird mit der Meldepflicht für das Datum gewährleistet, an dem die Patientin oder der Patient über die eigenen Rechte informiert wurde.

Im April 2021 forderte das Eidgenössische Departement des Inneren den Kanton Zürich zur Stellungnahme im Vernehmlassungsverfahren zur Revision der Verordnung über die Registrierung von Krebserkrankungen auf. Die Vernehmlassungsvorlage sah vor, diese Meldepflicht aufzuheben. Der Meldepflicht werde in der Praxis zu wenig Folge geleistet, hiess es in der Begründung. Das führe zu «ressourcenaufwendigen Nachforschungen» durch die Krebsregister.

Die Datenschutzbeauftragte setzte sich in ihrem Mitbericht zur Stellungnahme des Kantons Zürich für die Beibehaltung der Meldepflicht ein. Die geltend gemachten Vollzugsprobleme rechtfertigen keine Aufhebung dieser Meldepflicht. Sie offenbaren im Gegenteil, dass die Patienteninformationspflicht in der Praxis nicht genügend ernst genommen wird. Die Datenschutzbeauftragte verwies auf einen Vorschlag der Gesundheitsdirektion, wie die Meldepflicht besser eingehalten werden kann, etwa durch zusätzliche Information der Meldepflichtigen, also der Gesundheitseinrichtungen, der Ärztinnen und der Ärzte, sowie durch Androhung von aufsichtsrechtlichen Massnahmen.

Im nachfolgenden Beschluss des Bundesrates zur Teilrevision der Krebsregistrierungsverordnung wurde von der Aufhebung der Meldepflicht abgesehen. Die Meldepflicht liefert einen Beitrag dazu, dass betroffene Personen nur mit ihrem Wissen in das Krebsregister aufgenommen werden.

Getrübte Sicht auf die Cloud

Nicht nur die Pandemie hat den Hunger verstärkt, die bekanntesten Cloud-Produkte in der Verwaltung und in den Gemeinden einsetzen zu wollen. Das einfache Bedienen, die intelligenten Produkte, die schnelle Verfügbarkeit, aber auch die sichere Umgebung stärken noch immer das Wachstum bei Cloud-Dienstleistungen. Daraus ergeben sich Fragen, die die Datenschutzbeauftragte immer häufiger beantworten muss.

Kann Azure für ein Forschungsprojekt genutzt werden? Können Mitarbeitende der KESB Videokonferenzen mit Klientinnen und Klienten durchführen? Darf eine Schule Classtime einsetzen? Ist isTest geeignet, um alle Prüfungen zu erfassen? Können Gemeinden Microsoft 365 nutzen? Warum kann ein öffentliches Organ diese Produkte nicht uneingeschränkt nutzen?

Im privaten Bereich sind die Annehmlichkeiten dieser kleinen und grossen Tools bekannt. Die Frustrationsgrenze im öffentlichen Bereich ist schnell erreicht. Meist wird dabei vergessen, dass der Staat eine besondere Verantwortung für die Daten der Einwohnerinnen und Einwohner trägt. Sie übergeben ihre Daten dem Staat nämlich nicht freiwillig. Deshalb können öffentliche Organe ihre Verantwortung im Unterschied zu privaten Organisationen nicht delegieren.

Ein Spital wollte für ein Forschungsprojekt Daten in der Cloud-Plattform Azure speichern. Die Datenschutzbeauftragte prüfte den Vertrag mit dem Anbieter. Neben der Anwendung des schweizerischen Rechts und einem schweizerischen Gerichtsstand stellt sich die Frage, ob Daten in die USA transferiert werden, ob die Standardvertragsklauseln Anwendung finden und welche Sicherheitsmassnahmen umgesetzt werden. Die Daten sind zwar verschlüsselt, der Auftragnehmer ist jedoch im Besitz des Schlüssels. In diesem Fall hat sich herausgestellt, dass die Daten pseudonymisiert sind. Die Auslagerung ist unter diesen Voraussetzungen datenschutzkonform.

Eine Kindes- und Erwachsenenschutzbehörde (KESB) kann Videokonferenzen mit Teams durchführen, allerdings nicht in allen Fällen. Microsoft hat zwar keine Kenntnis des Gesprächsinhalts, speichert aber die Randdaten. Dadurch erfährt das Unternehmen, wer mit wem kommuniziert und unter Umständen auch das Thema der Besprechung. Deshalb ist die Nutzung für den internen Austausch verhältnismässig, sofern keine Dokumente gespeichert werden. Für die Kommunikation mit Klientinnen und Klienten kann Teams jedoch nicht eingesetzt werden. Schon die Tatsache, dass die KESB mit einer Person kommuniziert, kann ein besonderes Personendatum sein. Für solche Videokonferenzen ist auf ein anderes Produkt auszuweichen, beispielsweise auf Mymeeting oder Zoom mit einem Switch-Rahmenvertrag.

Personaldaten in der Cloud
Im Rahmen der Weiterentwicklung der HR-Informatik der kantonalen Verwaltung wurden die Verantwortlichen bereits in vergangenen Jahren datenschutzrechtlich beraten. In einem weiteren Schritt wurden analysierte Lösungsvarianten vorgestellt, um die bestehende SAP-Stäfa-Lösung abzulösen. Dabei handelte es sich um eine On-Premise-Variante und zwei unterschiedliche hybride Lösungsvarianten.

Gemeinsam mit dem Amt für Informatik (AFI) und Verantwortlichen der SAP Schweiz wurde die Frage der Anwendbarkeit des CLOUD Act und das damit zusammenhängende Risiko thematisiert. Die Datenschutzbeauftragte wies auf die Notwendigkeit einer Datenschutz-Folgenabschätzung (DSFA) hin. Eine DSFA hilft, die Risiken zu erkennen und Massnahmen zu definieren. Auch der CLOUD Act wird dabei berücksichtigt. Zwar ist der CLOUD Act auf europäische Anbieter wie SAP nicht anwendbar. Allerdings muss er in diesem Fall berücksichtigt werden, weil US-amerikanische Unterauftragsnehmer beteiligt sind oder ein Zugriff durch solche auf die Daten des Kantons erfolgen soll.

Auch für dieses Projekt des Personalamts sind die Publikationen der Datenschutzbeauftragten zum Thema Auslagerung zu berücksichtigen. Eine ausführliche und vollständige Vertragsausgestaltung ist ebenso unumgänglich wie die präzise Anpassung der Informationssicherheitsmassnahmen an die Art der Daten, das Land, in dem die Datenbearbeitung stattfindet, und das dortige Datenschutzniveau sowie die Transparenz in Bezug auf die Unterauftragsverhältnisse.

Im Rahmen der Kategorisierung der Daten ist zu entscheiden, welche Daten vor Ort gespeichert werden und welche Daten in die Cloud gehen sollen. Personalakten beinhalten besondere Personendaten wie Mitarbeiterbeurteilungen, Arztzeugnisse und auch Strafregisterauszüge. Sie bedürfen einem besonderen Schutz.

USA ohne angemessenes Datenschutzniveau
Der Gerichtshof der Europäischen Union (EuGH) urteilte im Juli 2020, dass die USA trotz des Privacy-Shield-Abkommens kein Land mit angemessenem Datenschutzniveau sei. Das Schrems II genannte Urteil hat Auswirkungen auf die Schweiz. Auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) strich die USA von der Liste der Länder mit angemessenem Datenschutzniveau.

Die meistgenutzten Cloud-Produkte stammen jedoch von US-amerikanischen Firmen und ein Transfer von Personendaten in die USA ohne zusätzliche Massnahmen war aufgrund des Urteils rechtswidrig. Der EDÖB anerkannte inzwischen die neuen Standardvertragsklauseln der Europäischen Kommission vom Juni 2021. Sie können als Grundlage für die Übermittlung von Personendaten in die USA und andere Länder mit nicht angemessenem Datenschutzniveau eingesetzt werden. Die Standardvertragsklauseln müssen an das schweizerische Recht angepasst respektive ergänzt werden, indem Module ausgewählt, die zuständige Aufsichtsbehörde benannt, schweizerisches Recht für vertragliche Ansprüche und ein schweizerischer Gerichtsstand festgehalten werden. Diese Klauseln mögen zwar nur ein Papier sein, sind aber dennoch wichtig. Allerdings müssen öffentliche Organe weitere Massnahmen umsetzen, wenn sie ein Produkt aus den USA nutzen wollen. Weitere Details finden sich auf der Website der Datenschutzbeauftragten.

Vorgehen bei der Wahl eines Cloud-Produkts
Die Datenschutzbeauftragte hat die Leitfäden Bearbeiten im Auftrag, Verschlüsselung im Rahmen der Auslagerung und Auslagerung unter Berücksichtigung des CLOUD Act publiziert. Die rechtlichen, organisatorischen und technischen Anforderungen bei der Nutzung von Cloud-Dienstleistungen sind also bekannt. Trotzdem verunsichert die Entscheidung, Daten in die Cloud auszulagern, Mitarbeitende öffentlicher Organe. Deshalb muss in jedem Fall strukturiert vorgegangen werden. Der Weg zum richtigen Produkt und dessen sicheren Nutzung führt über die richtigen Fragen, die gestellt werden müssen, eine sorgfältige Risikoanalyse unter Einbezug aller möglichen Varianten und die Prüfung von Alternativen. Dabei gilt es, auch die Neuerungen in Praxis und Technik zu berücksichtigen. Die Abklärungen sind komplex und umfangreich. Eine Datenschutz-Folgenabschätzung kann Klarheit geben. Die entsprechenden Formulare sind auf der Website der Datenschutzbeauftragten www.datenschutz.ch verfügbar.

Vor der Auswahl eines Produktes muss festgelegt werden, welche Daten bearbeitet werden sollen. Sind besondere Personendaten dabei? Müssen Berufsgeheimnisse berücksichtigt werden? Aufgrund der Liste der bearbeiteten Daten können mit den Leitfäden der Datenschutzbeauftragten die notwendigen Massnahmen zum Schutz der Informationssicherheit bestimmt werden. Erst jetzt kann ein Produkt ausgewählt werden. Nun muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Zeigt sich, dass mit dem Projekt besondere Risiken verbunden sind, muss es der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden. Weitere Schritte sind eine rechtliche und technische Überprüfung der Verträge. Auch oder erst recht, wenn die Daten in der Cloud sind, müssen Massnahmen vor Ort umgesetzt werden, bevor das Produkt genutzt werden kann. Dazu gehören etwa die Kategorisierung der Daten, die Bestimmung der Zugriffsberechtigungen, die Wahl des Speicherortes sowie die Verschlüsselung.

Die beschriebenen Abklärungen können zum Resultat führen, dass ein gewähltes Produkt mit bestimmten Daten nicht genutzt werden kann. Das öffentliche Organ trägt immer die alleinige Verantwortung für den Schutz der Daten. Sie kann nicht durch eine Einwilligung auf die Einwohnerinnen und Einwohner übertragen werden. Das öffentliche Organ kann mit technischen Massnahmen einige Schwachstellen eines Produkts beheben, etwa mit der Verschlüsselung der Daten und dem Schlüsselmanagement beim öffentlichen Organ. Oft verhindert dies jedoch die Nutzung der gewünschten Funktionalitäten. Eine Speicherung der Daten vor Ort statt in der Cloud kann als Lösung infrage kommen. Diese Massnahme löst die Schwierigkeiten allerdings nur zeitlich begrenzt, denn die Hersteller werden ihre Produkte zukünftig als reine Online-Lösungen anbieten. Ein Beispiel für diese Entwicklung ist das Produkt Skype for Business von Microsoft, das an vielen Orten standardmässig für die Telefonie eingesetzt wurde. Hier war die lokale Speicherung der Randdaten möglich. Die Unterstützung dieses Produkts wird jedoch eingestellt. Beim Nachfolgeprodukt Teams werden die Randdaten in jedem Fall beim Anbieter gespeichert. Randdaten können in bestimmten Fällen Aufschluss über die persönliche, wirtschaftliche oder strafrechtliche Situation der Kontaktperson geben.

Bei der Auslagerung von Datenbearbeitungen können unter diesen Umständen verschiedene weitere Massnahmen ergriffen werden. So kann die Nutzung eines Produkts für bestimmte Daten eingeschränkt werden, etwa für Daten unter besonderen Geheimnispflichten. Andere Lösungsideen sind eine hybride Cloud, bei der bestimmte Daten vor Ort gespeichert werden. Auch eine treuhänderische Cloud steht zur Diskussion. Alternativen sind in Open-Source-Produkten oder einer eigenen Cloud-Lösung zu finden.

Die Sicherheitspolitische Kommission des Nationalrats erachtet es als notwendig, eine kantons- und organübergreifende digitale schweizerische Infrastruktur mit Cloud-Diensten zu schaffen, um dem Schutz der Daten gerecht zu werden. In der Europäischen Union laufen Bestrebungen zur digitalen Souveränität. Bis zur definitiv datenschutzkonformen Umsetzung wird es aber noch dauern.

Rahmenverträge regeln meist nur Kernelemente

Rahmenverträge beinhalten Minimummassnahmen zum Schutz der Daten und entbinden die öffentlichen Organe zumindest in einigen wichtigen Bereichen davon, einzeln zu verhandeln. Rahmenverträge bestehen für Apple Classroom, Microsoft 365 im Bildungsbereich und Google Workspace in den Schulen. Zurzeit verhandelt die Schweizerische Informatikkonferenz (SIK) die Rahmenverträge zur Nutzung dieser Produkte in der Verwaltung mit Microsoft neu. Diese Verträge halten mindestens einen schweizerischen Gerichtsstand und das anwendbare schweizerische Recht fest. Weiter können sie auch die Speicherorte, die Kontrollrechte, die Bearbeitung der Daten für Zwecke des Produkteanbieters und vieles mehr regeln. Meistens sind sie jedoch nicht sehr umfangreich und beschränken sich auf die Kernelemente, da nur für diese ein Konsens gefunden werden kann.

Die restlichen Vertragspunkte wie Umfang und Art der Datenbearbeitung, Datenbekanntgabe an Dritte, Meldepflicht, Datenportabilität, Informationssicherheitsmassnahmen wie Verschlüsselung oder Zwei-Faktor-Authentifizierung sind individuell zu regeln. Vielfach werden diese in den AGB festgehalten. Diese sind genauestens zu prüfen. Auch mächtige Marktführer müssen die gesetzlichen Anforderungen erfüllen. Das öffentliche Organ kann sich seiner Verantwortung für den Schutz der Daten auch bei der Auslagerung nicht entziehen.

Für jede Datenbearbeitung muss die Nutzung eines Cloud-Produktes individuell geprüft werden. Besondere Personendaten brauchen besonderen Schutz. Daten unter besonderen Geheimnispflichten gehören nicht in eine Cloud, die ausländischen Behörden unter Umgehung des Rechtshilfeweges unter bestimmten Voraussetzungen Zugang gewähren (CLOUD Act). Dies trifft beispielsweise auf Steuerdaten oder Daten unter einem Berufsgeheimnis zu.

Verführerisches Datenmeer

Mit dem Einsatz neuer Technologien fallen immer grosse Datenmengen an. Wo eine grosse Menge an Personendaten vorhanden ist, wecken diese Begehrlichkeiten. Dadurch steigt die Gefahr für eine Grundrechtsverletzung der betroffenen Personen.

Grenzen der Überwachung bei Online-Prüfungen
In Zeiten von Corona ersetzten Universitäten und Hochschulen Präsenzprüfungen durch Online-Prüfungen. Die Prüfungsaufsicht musste angepasst werden. Dafür wurde oft sogenannte Proctoring-Software eingesetzt, die erheblich in die Grundrechte der Studierenden eingreift. Verunsicherte Studierende, aber auch Medien wandten sich an die Datenschutzbeauftragte.

Zur Überwachung von Online-Prüfungen existieren verschiedene Methoden und Programme. Sie alle bearbeiten eine grosse Menge an Personendaten und greifen stark ein in das Grundrecht der informationellen Selbstbestimmung der Studierenden. Die Intensität des Eingriffs ist abhängig von den im Einzelfall eingesetzten Funktionen. Diese reichen von Echtzeitüberwachung mit einem Videokonferenzprogramm bis zur softwaregesteuerten Aufzeichnung und Analyse des Nutzerverhaltens (Filmen, Gesichts- und Stimmerkennung, Pupillenbewegungen, Tastatur- und Mausnutzungsverhalten). Einzelne Programme verbieten virtuelle Hintergrundbilder, sodass auch Einblicke in die privaten Wohnräume übertragen oder aufgezeichnet werden. Dies stellt einen Eingriff in das Grundrecht auf Achtung der Wohnung dar. Für die Studierenden ist zudem nicht nachvollziehbar, wie der Algorithmus ihr Verhalten analysiert und welche Schlüsse daraus gezogen werden.

Die Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) setzte zur Überwachung von Online-Prüfungen die Software Proctorio ein. Diese ist als Browser-Add-on konzipiert und verlangt die Verwendung bestimmter Browser sowie die Installation des Add-on auf dem privaten Computer der Studierenden. Die Software verlangt weitgehende Zugriffe auf Kamera, Mikrofon und weitere Funktionen. Sie erhält dadurch zusätzliche Informationen von den Geräten und damit auch über die Studierenden selber.

Aus grundrechtlicher Sicht ist massgebend, dass für den Einsatz einer solchen Software eine Rechtsgrundlage besteht, ihr Einsatz im öffentlichen Interesse erfolgt und verhältnismässig ist (Art. 36 BV). Die Datenschutzbeauftragte prüft, ob Proctorio durch die ZHAW datenschutzkonform eingesetzt werden kann. Dazu steht sie im engen Austausch mit der ZHAW. Die Überprüfung ist noch nicht abgeschlossen. Nach Abschluss wird die Datenschutzbeauftragte über das Ergebnis orientieren.

Andere Hochschulen zeigten, dass auch weniger einschneidende Möglichkeiten bestehen, die faire und regelkonforme Prüfungen gewährleisten. Einige haben die Prüfungen angepasst und setzen auf Open-Book-Prüfungen. Wo dies nicht möglich ist, werden andere digitale Mittel eingesetzt. So haben sich einige für die Echtzeitüberwachung durch ein Videokonferenzprogramm entschieden. Da die Aufnahmen nicht gespeichert und durch Algorithmen analysiert werden, ist der Eingriff in die informationelle Selbstbestimmung deutlich weniger einschneidend.

ZVV-Check-in-Funktion und der Zugang zu riesigen Datenmengen

Seit 2018 verfügt die ZVV-Ticket-App über eine Check-in-Funktion. Die oder der Reisende kann vor der Reise ein- und nach der Reise wieder auschecken. Anschliessend wird der Preis in Rechnung gestellt. Der bisherige Anbieter des Systems stellt den Betrieb ein. Das einzige Alternativsystem wird durch das private Unternehmen Fairtiq angeboten. Der ZVV legte das Vorhaben der Datenschutzbeauftragten zur Vorkontrolle vor. Sie stellte fest, dass für das Vorhaben eine ausreichende Rechtsgrundlage besteht. Die Aufbewahrungsfristen sind von fünf Jahren auf zwölf Monate zu kürzen. Die vertraglichen Bestimmungen sind den kantonalen Vorgaben in den AGB Auslagerung Informatikleistungen anzupassen. Die Datenschutzbeauftragte kann aufgrund der ihr vorliegenden Informationen nicht abschliessend beurteilen, ob für das vorgesehene Vorgehen zur Betrugsbekämpfung eine ausreichende Rechtsgrundlage besteht. Zur Betrugsbekämpfung werden Personendaten aufbewahrt, um Muster von Fehlverhalten erkennen zu können. Dafür werden auch die Angaben aus Apps anderer öffentlicher Verkehrsbetriebe abgeglichen. Werden Muster von Fehlverhalten festgestellt, wird die nutzende Person in allen Apps gesperrt. Diese Möglichkeit besteht erst, seitdem Fairtiq einziger Anbieter der Check-in-Funktion ist. Die Verbindung der Daten ist eine neue zusätzliche Datenbearbeitung.

Ein ZVV-Kunde bat die Datenschutzbeauftragte, die Zugriffsberechtigungen der ZVV-App im Zusammenhang mit der Check-in-Funktion zu überprüfen. Für die Nutzung der Funktion muss der permanente Zugriff der App auf den Standort der Person erlaubt werden. Die Option «Beim Verwenden der App» reicht nicht aus. Der Zugriff auf aktuelle Standortdaten ist sehr heikel. Ihre Verknüpfung führt zu einem Bewegungsprofil. Dadurch werden die Daten zu besonderen Personendaten, für die zusätzliche Schutzmassnahmen vorzusehen sind.

Die Datenschutzbeauftragte hatte bei der Vorabkontrolle festgestellt, dass für die Check-in-Funktion eine Rechtsgrundlage besteht. Allerdings ging sie davon aus, dass nur während der Nutzung der Funktion Daten bearbeitet würden. Durch den permanenten Zugriff werden Daten bearbeitet, auch wenn die App geöffnet ist, die Funktion aber aktuell nicht genutzt wird. Die Datenschutzbeauftragte beurteilt dies als unverhältnismässig. Die Verantwortung für diese Bearbeitung kann nicht auf die Nutzenden der App übertragen werden. Die Check-in-Funktion des bisherigen Anbieters konnte auch ohne permanenten Standortzugriff genutzt werden.

Einblicke in private Räume im Internet

Im Frühjahr 2021 fragte das Amt für Abfall, Wasser, Energie und Luft (AWEL) die Datenschutzbeauftragte, ob die Aufschaltung der Schrägluftbilder im GIS-Browser aus datenschutzrechtlicher Sicht unproblematisch sei. Mit den Schrägluftbildern der Seeufer des Zürichsees sollen allfällige Veränderungen an der Seeuferlinie erkannt werden. Die Bilder waren zu diesem Zeitpunkt bereits seit mehreren Wochen im GIS-Browser aufgeschaltet und so im Internet frei zugänglich.

Bei der stichprobeweisen Überprüfung stellte die Datenschutzbeauftragte fest, dass die hochauflösenden Bilder weitgehende Einblicke in Wohn- und Schlafzimmer, in Wintergärten sowie auf Balkone und Terrassen ermöglichten. Auch wenn auf den Bildern keine Personen identifiziert werden konnten, ermöglichte die hohe Auflösung der Bilder Einblicke in private Räume und damit in Grundrisse und Raumnutzungen der Liegenschaften.

Die Datenschutzbeauftragte wies darauf hin, dass dies einen Eingriff in die Privatsphäre der betroffenen Personen darstellt. Für das Zugänglichmachen der Bilder über einen Downloaddienst ist zwar eine Rechtsgrundlage vorhanden. Eine Rechtsgrundlage gibt aber noch nicht das Recht zu einer Datenbearbeitung. Eine Datenbearbeitung durch öffentliche Organe muss immer auch verhältnismässig sein. Sie muss geeignet und nötig sein, um einen bestimmten Zweck zu erreichen. Kann der Zweck auch mit weniger weitgehenden Massnahmen erreicht werden, sind diese zu wählen. Im vorliegenden Fall dienten die Bilder einem verwaltungsinternen Zweck. Verwaltungsmitarbeitende sollen damit Veränderungen der Seeuferlinie erkennen und allfällige Massnahmen ergreifen können. Dafür müssen die Daten nur ihnen zur Verfügung stehen. Eine Veröffentlichung im Internet erwies sich als unverhältnismässig. Die zuständige Verwaltungsabteilung veranlasste darauf, dass die Schrägluftbilder nur noch verwaltungsintern zur Verfügung stehen.

Ungewollter «Beifang»
Im Rahmen eines anderen Projektes wurden Kameras an einer Brücke über die Limmat montiert, um den Kunststoffabfall zu analysieren, der unter der Brücke durchfliesst. Die Datenschutzbeauftragte prüfte das Konzept im Hinblick auf die Aufnahmen von Personen. Da im Aufnahmebereich der Kameras ein Schwimmverbot herrscht und auch die Passagierschiffe nicht erfasst wurden, lag keine Bearbeitung von Personendaten vor. Die Datenschutzbeauftragte prüfte zudem die geplanten Massnahmen für den Fall, dass das Schwimmverbot missachtet wird oder ein Passagierschiff ein unvorhergesehenes Manöver fahren muss. Die für diesen Fall vorgesehenen Massnahmen hielt die Datenschutzbeauftragte für angemessen (nachträgliche Anonymisierung, manuelle Löschung und eine kurze Aufbewahrungsdauer).

Wo Personendaten vorhanden sind, wird gerne nachgefragt
Eine Einwohnerkontrolle erkundigte sich bei der Datenschutzbeauftragten, ob sie einer Liegenschaftsverwaltung den Zivilstand einer bestimmten Mieterin bekannt geben dürfe, damit die Kündigung rechtsgültig zugestellt werden könne. Die Datenschutzbeauftragte hielt fest, dass der Zivilstand einer Einwohnerin oder eines Einwohners gestützt auf die Bestimmungen des Gesetzes über das Meldewesen und die Einwohnerregister (MERG) bekannt gegeben werden dürfe, wenn ein berechtigtes Interesse besteht und kein überwiegendes Interesse entgegensteht. Sie wies darauf hin, dass die Auskunft über eine Person nicht dazu missbraucht werden darf, Informationen über eine andere Person zu erhalten, im konkreten Fall über den vermuteten Ehepartner der Mieterin.

In einem anderen Fall wollte eine Liegenschaftsverwaltung Auskunft darüber, ob Bewohnerinnen und Bewohner einer Liegenschaft einen Hund halten, da sie dies nicht erlaube. Die Datenschutzbeauftragte riet der Einwohnergemeinde, die Liegenschaftsverwaltung zu fragen, welche gesetzliche Grundlage für ihre Anfrage vorliege. Das Hundegesetz regelt die Anmeldung von Hunden bei der Einwohnergemeinde. Es sieht jedoch nicht vor, dass diese Daten an Liegenschaftsverwaltungen oder andere Private bekannt gegeben werden.

Die Datenschutzbeauftragte hat zum Entwurf des Gesetzes über den selbstbestimmten Leistungsbezug durch Menschen mit Behinderung (Selbstbestimmungsgesetz) Stellung genommen. Das Gesetz führt zu einem Systemwechsel von der Objektfinanzierung hin zur Subjektfinanzierung. Die Datenschutzbeauftragte wies darauf hin, dass dieser Systemwechsel die systematische Erhebung von sensitiven Personendaten bis hin zu Persönlichkeitsprofilen der Leistungsberechtigten mit sich bringt. Der Entwurf sah sehr weitgehende Zugriffsrechte für Behörden vor, die diese Personendaten für die Erfüllung ihrer Aufgaben nicht benötigen. Die Datenschutzbeauftragte stellte klar, dass die Einhaltung der datenschutzrechtlichen Grundsätze, besonders die Verhältnismässigkeit, auch in der Gesetzgebung zu beachten und in diesem Zusammenhang von besonderer Bedeutung ist.

Die Anregungen der Datenschutzbeauftragten zu Verbesserungen im Erlass wurden übernommen. Die Datenschutzrechte der betroffenen Personen werden im Selbstbestimmungsgesetz nun gewahrt.

Statistik zur finanziellen Situation der Zürcher Haushalte

Gestützt auf einen politischen Vorstoss erstellt das Statistische Amt (STAT) einen neuen Datensatz für den Kanton Zürich. Dieser erlaubt eine Einschätzung der finanziellen Situation der Haushalte. Dafür verknüpft das STAT eine Vielzahl von Personendaten aus verschiedenen Quellen auf Kantons- und Bundesebene miteinander. Der Datensatz enthält Informationen zu mehreren Hunderttausend Haushalten. Bei der Verknüpfung dieser Informationen besteht die Möglichkeit, dass Persönlichkeitsprofile erstellt werden und daraus neue Zusammenhänge über einzelne Personen erschlossen werden. Eine Datenverknüpfung in diesem Ausmass stellt hohe Anforderungen an den Datenschutz. Die Datenschutzbeauftragte hat das Vorhaben daher im Rahmen einer Vorabkontrolle geprüft.

Gestützt auf die ihr vorgelegten Unterlagen stellte sie fest, dass für die geplanten Datenbezüge aus den verschiedenen Quellen ausreichende Rechtsgrundlagen bestehen. Die Daten werden ausschliesslich zu statistischen Zwecken genutzt. Eine andere Nutzung der Daten wäre mit dem Grundsatz der Zweckbindung nicht vereinbar. Die Datenschutzbeauftragte wies in ihrem Bericht darauf hin, dass auch bei der Bearbeitung einer grossen Datenmenge der Grundsatz der Verhältnismässigkeit einzuhalten ist. Nur die Daten dürfen bearbeitet werden, die zur Erstellung der geplanten Modelle geeignet und erforderlich sind. Die Datenschutzbeauftragte führte die noch zu erfüllenden technischen und organisatorischen Anforderungen in ihrem Bericht auf.

Durch den frühen Einbezug der Datenschutzbeauftragten und den kontinuierlichen Austausch mit den Projektverantwortlichen konnten die datenschutzrechtlichen Anliegen von Anfang an berücksichtigt werden.

Ohne Datenschutz keine Demokratie

Wie damals die Industrialisierung stellt heute die Digitalisierung die Grundlagen der Gesellschaft infrage. Die Datenschutzbeauftragte zeigt mit ihren Anstrengungen in den Bereichen Kommunikation und Aus- und Weiterbildung auf, dass Datenschutz nie ein Selbstzweck ist. Er fördert Lösungen, die unsere freiheitliche Gesellschaftsform respektieren.

Kurz und deutlich – 20 Sekunden mit klarer Botschaft

Das Argument, dass der Datenschutz einer guten Lösung im Wege steht, ist schnell zur Hand. Das war schon vor der Corona-Pandemie so. Die Datenschutzbeauftragte produzierte vier Spots von je 20 Sekunden, die die Bedeutung des Schutzes der Privatsphäre für jede und jeden illustrieren. «Der Datenschutz schützt meine Privatsphäre und das bedeutet, dass ich meine Meinung frei und ohne Angst äussern kann. Nur so ist Demokratie möglich», ist eine der Aussagen. Eine andere: «Ich weiss nicht, was mit meinen Informationen im Netz geschieht. Es kann sein, dass meine Daten missbraucht werden und ich manipuliert werde.» Die vier Spots sind auf dem datenschutzkonformen schweizerischen Videoportal Switchtube publiziert und auf der Website der Datenschutzbeauftragten www.datenschutz.ch eingebunden. Sie können in HD-Auflösung und Kinoqualität bei der Datenschutzbeauftragten angefordert werden.

Filme in wissenschaftlichem und gesellschaftlichem Kontext

Stehen sich Datenschutz und investigativer Journalismus im Weg? Wie schützt investigativer Journalismus die Privatsphäre? Oder auch: Überlebt die demokratische Gesellschaft die Künstliche Intelligenz (KI)? Können wir noch kontrovers diskutieren, wenn Algorithmen alles für uns vorsortieren und uns in eine Wohlfühlblase einpacken? Ab Herbst 2021 konnte die Datenschutzbeauftragte ihre Publikumsveranstaltungen wieder aufnehmen. Neben einem ZFF Talk am Zurich Film Festival organisierte die Datenschutzbeauftragte im Jahr 2021 zwei Filmabende im Kino Kosmos. Nach dem Film «Ich bin dein Mensch» von Maria Schrader stellte der Journalist Simon Jacoby die ketzerische Frage: «Warum sollten wir an der Demokratie festhalten, wenn das Volk ständig gegen seine eigenen Interessen entscheidet? KI brächte vielleicht bessere Entscheidungen zustande.» Die Geschäftsleiterin der Stiftung für Technologiefolgen-Abschätzung Dr. Elisabeth Ehrensperger antwortete: «Entscheide müssen vom Volk dann auch mitgetragen werden.» KI könnte auf den ersten Blick vermeintlich vernünftigere Lösungen bringen als Volksabstimmungen. Sie würden von der Bevölkerung aber als Zwangsmassnahmen begriffen und deshalb nicht akzeptiert. Weiter meinte sie: «Die Geschwindigkeit der Technologieentwicklung passt wahrscheinlich nicht zur Art, wie menschliche Entscheidungsprozesse ablaufen.»

Social-Media-Daten für die Forschung
Für das Digital Festival 2021 spannte die Datenschutzbeauftragte mit der Kantonalen Ethikkommission (KEK) und dem Institut für Kommunikationswissenschaft und Medienforschung der Universität Zürich zusammen. In einem Lab diskutierten die Datenschutzbeauftragte Dominika Blonski, der Geschäftsführer der KEK Peter Kleist und Professor Thomas Friemel, Leiter der Abteilung Mediennutzung und Medienwirkung, mit den Digital-Festival-Besucherinnen und -Besuchern über die Möglichkeiten und Grenzen der Nutzung von Social-Media-Daten in der Forschung. Social Media oder auch Dating Apps sind eine Art unkontrolliertes Sozialexperiment. Die Nutzerinnen und Nutzer publizieren freiwillig – teils absichtlich, teils unwissentlich – Unmengen an Informationen und die Techfirmen werten diese detailliert aus. Anhand konkreter Beispiele aus der Forschungspraxis wurden Wege gesucht, die die Teilhabe der Wissenschaft ermöglichen. Dabei wurde thematisiert, wie vulnerable Personen geschützt werden können oder ob eine Anonymisierung solcher Daten überhaupt möglich ist.

Sichtbare Unabhängigkeit und besser zugängliche Informationen
Im Sommer 2021 lancierte die Datenschutzbeauftragte ihre neue Website www.datenschutz.ch. Sie bekräftigt damit die Unabhängigkeit ihrer Behörde.

Die Datenschutzbeauftragte stellt auf ihrer Website einen grossen Informationsschatz zu vielen Aspekten des Datenschutzes und der Informationssicherheit zur Verfügung. Die Flaggschiffe dieser aufbereiteten Beratungstätigkeit sind die Datenschutzlexika mit schnellen Antworten für den Alltag in Volksschulen, Mittel- und Berufsfachschulen sowie in Einwohnerkontrollen. Bisher waren die Inhalte als PDFs publiziert. Neu sind sie als HTML-Seiten zugänglich. Einzelne Artikel können nun direkt verlinkt und weitergegeben werden. Die aktuellste Version der kompletten Lexika oder einzelner Artikel können direkt ab der Website als PDF exportiert werden. Auch die Inhalte der Leitfäden und Merkblätter sind dank der intelligenten Suchfunktion auf www.datenschutz.ch viel besser auffindbar.

Die datenschutzkonforme Gestaltung einer Website eines öffentlichen Organs kann herausfordernd sein. Die Datenschutzbeauftragte hat keine Abkürzungen gewählt. Bei der Einbindung externer Dienste etwa für die Suche und die PDF-Erstellung gehen keine Daten der Besucherinnen und Besucher der Website weiter an die Anbieter der Funktionen.

Auch für die Illustration wählte die Datenschutzbeauftragte einen unabhängigen Weg. Bei Themen des Datenschutzes und der Informationssicherheit werden meist generische Bilder von Smartphones, Tastaturen und Hackern in Kapuzenpullovern oder Stimmungsbilder aus dem Kanton gewählt. Stattdessen beauftragte die Datenschutzbeauftragte den preisgekrönten Schweizer Fotografen Jean-Vincent Simonet. Er schuf eine Bilderwelt, die die digitale Welt, den Kontrollverlust der Menschen und ihr Bedürfnis nach Schutz dokumentiert. «Die künstlerische Bearbeitung vermittelt ein starkes und farbenfrohes, aber auch beunruhigendes Gefühl: Überall im Kanton Zürich ist jeder Mensch mit dem Schutz der Privatsphäre und dem Datenschutz konfrontiert», schreibt Simonet.

Die neue Website gibt der Behörde die Möglichkeit, dem gesetzlichen Auftrag zur Information über die Anliegen des Datenschutzes und des Schutzes der Privatsphäre noch besser gerecht zu werden.

Zweites Corona-Jahr – die Datenschutzbeauftragte bleibt flexibel

Die Datenschutzbeauftragte hat 2021 ihr bewährtes Angebot an Aus- und Weiterbildungsveranstaltungen durchführen können. Dazu kamen Angebote, die auf die Bedürfnisse von Kundinnen und Kunden zugeschnitten wurden. Die Schwerpunkte lagen im Sozialbereich, bei den Gemeinden im Einwohnerkontrollwesen, bei den Schulen sowie bei der klinischen Forschung in Spitälern. Je nach Thema und Bedarf führte die Datenschutzbeauftragte die Aus- und Weiterbildungsveranstaltungen interdisziplinär durch.

An zwei Fachseminaren für Mitarbeitende der Einwohnerkontrollen hat die Datenschutzbeauftragte die fachspezifischen datenschutzrechtlichen Anforderungen erläutert. Die Teilnehmenden wünschten für künftige Fachveranstaltungen mehr Zeit für die Auseinandersetzung mit konkreten Alltagsfragen. Die Datenschutzbeauftragte sieht dies als Hinweis dafür, dass der Umgang mit datenschutzrechtlichen Themen im Verwaltungsalltag verunsichert und ihr Weiterbildungsangebot einem grossen Bedürfnis entspricht.

Auch in diesem Jahr war die Datenschutzbeauftragte am CAS Kindes- und Erwachsenenschutz und am CAS Sozialhilfe der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) beteiligt. Die ganztägigen Lehrveranstaltungen bieten Zeit, um die datenschutzrechtlichen Themen im Sozialbereich zu vertiefen und anhand praktischer Fälle zu analysieren. Für eine Institution im Sozialbereich führte die Datenschutzbeauftragte ein Seminar durch, dessen Inhalt vollständig auf die datenschutzrechtlichen Anforderungen im Arbeitsalltag ihrer Mitarbeitenden abgestimmt war. Unter den Teilnehmenden befanden sich hauptsächlich Sozialpädagoginnen und -pädagogen sowie Kleinkindererzieherinnen und -erzieher.

Die Auswirkungen der Corona-Krise und die fortschreitende Digitalisierung forderten die Schulen und Lehrpersonen auch im Jahr 2021 heraus. Die Datenschutzbeauftragte beteiligte sich wiederum am CAS Digital Leadership in Education der Pädagogischen Hochschule Zürich (PHZH). Sie informierte die Lehrpersonen einer Schule zu Datenschutzfragen an den Schulen.

Der CAS Datenschutzverantwortliche an der ZHAW ist fester Bestandteil der Aus- und Weiterbildungstätigkeit der Datenschutzbeauftragten. Er wurde auch im Jahr 2021 wieder zweimal durchgeführt. Diese Weiterbildung liefert eine solide Grundlage zu Datenschutzthemen und erfreut sich weiterhin grosser Nachfrage.

Ergänzt wurde das umfangreiche Angebot durch Referate an verschiedenen Veranstaltungen. Dabei standen Themen aus der Polizeitätigkeit im Vordergrund. So referierte die Datenschutzbeauftragte am Anlass der Parlamentarischen Gruppe für Polizei- und Sicherheitsfragen zum Thema DNA-Phänotypisierung oder am Forum Innere Sicherheit des Verbandes Schweizerischer Polizei-Beamter (VSPB) zum Thema Digitalisierung im Polizeibereich. Bei ihrem Besuch beim Jugendparlament erfreute sich die Datenschutzbeauftragte am lebhaften Austausch und am Engagement, das die Mitglieder für Fragen rund um Digitalisierung und Datenschutz in Schulen zeigten.

Auch das zweite Jahr der Corona-Krise erforderte von der Datenschutzbeauftragten Flexibilität. Ihre Weiterbildungsveranstaltungen wurden je nach Pandemielage und Corona-Schutzmassnahmen virtuell oder vor Ort abgehalten.

Impressum

Herausgeberin
Datenschutzbeauftragte des Kantons Zürich, Postfach,
8090 Zürich

Korrektorat
Text Control, Dufourstrasse 107, 8008 Zürich

Layout
TKF Kommunikation & Design, t-k-f.ch

Der Tätigkeitsbericht 2021 ist elektronisch verfügbar
unter www.datenschutz.ch/tb2021.

ISSN 2571-5003

Kontakt

E-Mail
datenschutz@dsb.zh.ch

Adresse
Datenschutzbeauftragte des Kantons Zürich,
Postfach, 8090 Zürich

Telefon
+41 43 259 39 99

Website
www.datenschutz.ch

Twitter
@dsb_zh

Youtube

Datenschutz mit Qualität