Stadt Zürich
Datenschutzstelle

2020

Gemäss § 39 des kantonalen Gesetzes über die Information und den Datenschutz (IDG; LS 170.4) berichtet die oder der Datenschutzbeauftragte dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht.

Der vorliegende Bericht bezieht sich auf das **Kalenderjahr 2020.**

Veröffentlicht werden die Berichte auf der **Webseite** der Datenschutzstelle der Stadt Zürich.

Zürich, anfangs Mai 2021
Marcel Studer, Datenschutzbeauftragter

Inhaltsverzeichnis

Grundlagen

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

Wer sind wir?

Die Datenschutzstelle der Stadt Zürich besteht aus dem Datenschutzbeauftragten, drei juristischen Mitarbeitenden und einer Sekretariatsmitarbeiterin. Insgesamt teilen wir uns drei Vollzeitstellen. Organisatorisch ist die Datenschutzstelle dem Gemeinderat, also dem Parlament der Stadt Zürich, zugeordnet. In der Aufgabenerfüllung ist die Datenschutzstelle **unabhängig und weisungsfrei.**

Was tun wir?

Bei der Stadtverwaltung Zürich arbeiten über 28 000 Angestellte in neun Departementen mit insgesamt über 50 Dienstabteilungen. So vielfältig und unterschiedlich die Aufgaben und Tätigkeiten der Stadtverwaltung sind, eine Gemeinsamkeit besteht dennoch, die die meisten Angestellten teilen: Sie alle arbeiten mit Informationen, die sie beschaffen, weiterbearbeiten und mit anderen austauschen. Zahlreiche dieser Informationen betreffen uns Bürgerinnen und Bürger, Patientinnen und Patienten, Klientinnen und Klienten, Mitarbeiterinnen und Mitarbeiter in direkter oder indirekter Weise. Wann immer die Stadtverwaltung personenbezogene Informationen bearbeitet, gilt es, mit diesen richtig umzugehen.

Es gehört zu unseren wichtigsten Aufgaben, die Stadtverwaltung im Umgang mit Personendaten zu **beraten,** zu **unterstützen** und zu **kontrollieren.** Konkret gehören folgende Aufgaben zum Tätigkeitsbereich der Datenschutzstelle:

– **Projekte der Stadtverwaltung prüfen und beraten**
  Heutzutage gibt es kaum noch Daten, die nicht mittels moderner Informations- und Kommunikationstechnik (ICT) bearbeitet werden. In der Stadtverwaltung Zürich müssen sämtliche Projekte, die ICT betreffen, den sogenannten Informationssicherheits- und Datenschutz-Prozess (ISDS-Prozess) durchlaufen. Bei denjenigen Projekten, die aus datenschutzrechtlicher Sicht eine erhöhte Sensibilität aufweisen, führt die Datenschutzstelle eine sogenannte Vorabkontrolle durch. Dabei wird geprüft, ob die Rahmenbedingungen – in rechtlicher, organisatorischer und technischer Hinsicht – eingehalten werden. Bei weniger sensiblen Projekten steht nicht die Prüfung im Vordergrund, sondern vielmehr die Beratung durch die Datenschutzstelle.

  Im Berichtsjahr stellte die Stadtverwaltung der Datenschutzstelle via städtischem ISDS-Prozess **rund 70 Projekte oder Vorhaben** zur Prüfung und/oder Beratung zu. Eine so grosse Anzahl an Neuanmeldungen via ISDS-Prozess gab es bisher noch nie (was die Datenschutzstelle auch schon für das Jahr 2019 mit damals rund 60 Neuanmeldungen feststellen konnte).

– **Anfragen und Gesuche aus der Stadtverwaltung behandeln**
  Regelmässig wird die Datenschutzstelle von Rechtsdiensten oder Führungskräften der Stadtverwaltung gebeten, **Informationsbearbeitungen der Stadtverwaltung** aus datenschutzrechtlicher Optik zu beurteilen. Dabei geht es beispielsweise darum, ob Personendaten mit anderen Verwaltungsstellen ausgetauscht oder ob Informationen veröffentlicht werden dürfen, über welche Personendaten Auskunft zu erteilen oder wie bei Forschungsprojekten mit Personendaten umzugehen ist. Die Datenschutzstelle wird auch von Mitarbeitenden aus der Stadtverwaltung um Beratung oder Abklärung zu datenschutzrechtlichen Belangen in Zusammenhang mit dem Arbeitsplatz angefragt.

– **Anfragen und Gesuche von Privatpersonen beantworten**
  Wenden sich Privatpersonen mit Fragen oder Reklamationen an die Datenschutzstelle, führt dies oft zu umfangreichen Abklärungen. Bevor die Datenschutzstelle eine Beurteilung abgeben kann, müssen **Sachverhalt und Rechtslage** unter Mitwirkung der betroffenen städtischen Verwaltungsstellen **genau geklärt** werden. Solche «Anstösse von aussen» können Fehler oder Defizite bei Datenbearbeitungen in der Stadtverwaltung aufzeigen und zu entsprechenden Korrekturen führen.

– **Videoüberwachung der Stadtverwaltung überprüfen**
  Das Thema Videoüberwachung stellt für die Datenschutzstelle ein eigentliches **Schwerpunktthema** dar. In der Datenschutzverordnung der Stadt Zürich ist vorgeschrieben, dass städtische Verwaltungsstellen für ihre Videoüberwachungen Reglemente erlassen und diese der Datenschutzstelle zur Prüfung unterbreiten. Mittlerweile setzen mehrere städtische Verwaltungsstellen Videoüberwachungen ein und haben hierfür Reglemente erlassen. Der Beratungs- und Prüfungsaufwand der Datenschutzstelle in diesem Bereich ist gross, auch weil die Reglemente von Zeit zu Zeit angepasst werden müssen. Die Datenschutzstelle steht auch Privatpersonen für Auskünfte, Beratungen und Vermittlungen zur Verfügung. Weitere Ausführungen zum Thema Videoüberwachung folgen im entsprechenden FOKUS-Beitrag ab **Seite 38**.

– **Bei Stadtratsgeschäften und Gesetzgebungsverfahren mitwirken**
  Bei Anträgen an den Stadtrat, die Belange des Datenschutzes betreffen, wird die Datenschutzstelle zur **Stellungnahme** eingeladen. Werden rechtliche Grundlagen der Stadtverwaltung neu geschaffen oder angepasst und beinhalten diese auch datenschutzrechtliche Themen, ist die Datenschutzstelle regelmässig bereits in die entsprechenden Gesetzgebungsprojekte involviert.

– **Aus- und Weiterbildung durchführen**
  Das Datenschutzrecht betrifft das gesamte Spektrum der Stadtverwaltung und bringt aufgrund des gesellschaftlichen und technologischen Wandels immer wieder neue Fragestellungen mit sich. Es ist für die Mitarbeitenden der Stadtverwaltung wichtig, am Ball zu bleiben. Die Datenschutzstelle bietet Weiterbildungen an, die sich spezifisch auf die Bedürfnisse städtischer Verwaltungsstellen ausrichten. Auch die Mitarbeitenden der Datenschutzstelle nehmen regelmässig an Weiterbildungen teil.

Wie tun wir dies?

Die Datenschutzstelle ist Teil der Stadtverwaltung. Unser Handeln richtet sich nach dem Ziel, Datenschutz in der Stadtverwaltung wirkungsvoll umzusetzen. Datenschutz lässt sich aber nicht für alle Verwaltungsbereiche einheitlich realisieren. Datenschutz kann nur konkret und in Kenntnis der jeweiligen Situation umgesetzt werden. Um einen möglichst sachgerechten Umgang mit Daten erreichen zu können, bedarf es organisationsübergreifender und interdisziplinärer **Zusammenarbeit**. Insbesondere …

– **… mit den Verantwortlichen der Projekte und der Dienstabteilungen**
  Den «richtigen» Datenschutz erreicht man nur, wenn die konkreten Anforderungen und Gegebenheiten der jeweiligen Projekte und Verwaltungsbereiche verstanden und berücksichtigt werden. Der direkte Austausch mit den Projektverantwortlichen, Rechtsdiensten und Bereichsverantwortlichen ist deshalb äusserst wichtig.

– **… mit der Fachstelle für Informationssicherheit**
  Diese Fachstelle der städtischen Dienstabteilung Organisation und Informatik (OIZ) prüft alle ICT-Projekte auf die Einhaltung der Vorschriften zur Informationssicherheit. Die Prüfung erfolgt im Rahmen des erwähnten städtischen ISDS-Prozesses und in enger Koordination mit der Datenschutzstelle. Die Fachstelle für Informationssicherheit steht der Datenschutzstelle bei technischen Fragestellungen auch für weitere Abklärungen zur Verfügung.

– **… mit den Beraterinnen und Beratern für Datenschutz der Departemente**
  Alle städtischen Departemente verfügen über eine Beraterin oder einen Berater für Datenschutz. Diese erfahrenen Juristinnen und Juristen aus den Rechtsdiensten der Departementssekretariate beraten ihre Dienstabteilungen und sind für die Datenschutzstelle wichtige Ansprechpersonen. Unter der Leitung der Datenschutzstelle treffen sich die Beraterinnen und Berater der Departemente regelmässig zu Arbeitssitzungen und Weiterbildungen.

– **… mit Datenschutzbeauftragten der Kantone und des Bundes**
  Die Datenschutzbeauftragten der Kantone und des Bundes arbeiten über ihren schweizerischen Verband Privatim und dabei vor allem über thematische Arbeitsgruppen zusammen. Die Datenschutzstelle der Stadt Zürich ist in allen Arbeitsgruppen des Verbands vertreten.

In Zusammenarbeit mit den involvierten Verantwortlichen will die Datenschutzstelle **mit dienstleistungs- und lösungsorientiertem Handeln** erreichen, dass die Stadtverwaltung den Schutz der Grundrechte von Personen, über welche Daten bearbeitet werden, gewährleisten kann.

Das Datenschutzrecht kurz erklärt

In der Stadtverwaltung werden täglich zahlreiche Informationen bearbeitet: Telefongespräche werden geführt, E-Mails und Briefe erreichen und verlassen die Verwaltung, Dokumente und Dossiers werden in Papierform oder auf IT-Systemen gespeichert, geändert oder gelöscht, Datenbanken werden abgefragt und gefüttert, auf Webseiten oder über Social Media wird mit der Bevölkerung kommuniziert usw. usw. Doch wann kommt der Datenschutz ins Spiel? Und wie muss sich die Stadtverwaltung verhalten?

Personendaten als Anknüpfungspunkt

Das Datenschutzrecht kommt immer dann zur Anwendung, wenn die Stadtverwaltung **Personendaten** bearbeitet. Alle Informationen oder Angaben, die sich auf eine Person beziehen oder sich einer Person zuordnen lassen, stellen Personendaten dar. Dabei spielt es keine Rolle, in welcher Form diese Daten vorhanden sind (Wort, Bild, Ton) oder mit welcher Technik sie bearbeitet werden (analog oder digital). Die meisten Informationen, die in der Stadtverwaltung bearbeitet werden, sind Personendaten. Das Datenschutzrecht ist damit für die gesamte Stadtverwaltung grundsätzlich immer relevant.

Datenschutzrecht – aber welches?

Datenschutzgesetze werden in der Schweiz vom Bund, den Kantonen und zum Teil auch von den Gemeinden erlassen. Für die Stadtverwaltung ist in erster Linie das Datenschutzrecht des Kantons Zürich massgebend, konkret das **Gesetz über die Information und den Datenschutz (IDG)** und die dazugehörende Verordnung (IDV). Die Stadt Zürich kennt zusätzlich dazu eine eigene Datenschutzverordnung (DSV). Diese Verordnung ist vor allem für die Videoüberwachung durch städtische Verwaltungsstellen und den Datenbezug aus dem städtischen Einwohnerregister massgebend.

Was verlangt das Datenschutzrecht von der Stadtverwaltung?

Datenschutz ist ein **Grundrecht.** Die Verfassungen von Bund und Kanton verpflichten die Stadtverwaltung, bei der Bearbeitung von Personendaten Privatsphäre und Persönlichkeit der Bürgerinnen und Bürgern zu achten und zu schützen. Das IDG konkretisiert dieses Grundrecht, indem es für den Umgang mit Informationen Grundsätze und Prinzipien aufstellt, die rechtlicher, technischer und organisatorischer Natur sein können:

- **Gesetzmässigkeit:** Jede Tätigkeit der Verwaltung muss sich auf eine rechtliche Grundlage und somit auf einen Auftrag des Gesetzgebers abstützen können. Dies gilt auch für die Bearbeitung von Personendaten: Das Datenschutzrecht verlangt, dass die Verwaltung über eine genügende Berechtigung für die Datenbearbeitung verfügt. Ob und zu welchem Zweck die Stadtverwaltung Informationen über ihre Einwohnerinnen und Einwohner bearbeiten darf, ergibt sich aus den gesetzlichen Grundlagen der jeweiligen Verwaltungsbereiche: also beispielsweise aus der Polizei-, Sozialhilfe-, Gesundheits- oder Schulgesetzgebung.

- **Zweckbindung:** Die Verwaltung darf Personendaten nur zu dem Zweck bearbeiten, zu welchem sie erhoben worden sind. Jede Verwendung von Personendaten zu anderen Zwecken muss wiederum durch eine rechtliche Bestimmung oder durch eine Einwilligung der betroffenen Person gerechtfertigt sein.

- **Verhältnismässigkeit:** «Nicht mehr, als notwendig.» Dieser Grundsatz der Verhältnismässigkeit ist bei der Bearbeitung von Personendaten ganz besonders zu beachten. Er gilt nicht nur in Bezug auf den Umfang der Daten, sondern ist auch für die Festlegung der Löschfristen und Zugriffsrechte massgebend.

– **Informationssicherheit:** Personendaten sind vertraulich und müssen richtig und verfügbar sein. Durch Technologie und Organisation wie beispielsweise Verschlüsselung oder Zugriffskonzepte müssen Informationen geschützt werden. Welche Massnahmen konkret zu verlangen sind, ist abhängig von der Sensibilität der Daten, dem Verwendungszweck und dem Stand der Technik.

– **Transparenz:** Datenbearbeitungen der Verwaltung dürfen keine «black-box» sein. Sie müssen erkennbar, nachvollziehbar und verständlich sein. Das kann bedeuten, dass die Stadtverwaltung allenfalls über sensible Datenbearbeitungen adressatengerecht informieren und verbindliche Organisationsvorschriften erlassen muss.

Schwerpunkte

Digitalisierung der Stadtverwaltung

Für die Stadt Zürich hat die Digitalisierung der Stadtverwaltung grossen strategischen Stellenwert: Gemäss **Strategie Zürich 2035** gilt die «Digitale Stadt» als eines der Handlungsfelder für die Herausforderungen der Zukunft und in der **IT-Strategie der Stadt Zürich 2016** wird die Digitalisierung als eine der strategischen Stossrichtungen bezeichnet. Mit Hilfe der Digitalisierung soll der Austausch mit der Bevölkerung, den Unternehmen und weiteren Anspruchsgruppen vereinfacht und schneller und komfortabler gestaltet werden. Darüber hinaus soll die Digitalisierung verwaltungsintern die effizientere Gestaltung von Prozessen ermöglichen.

Erkenn- und erlebbar wird die Digitalisierung der Stadtverwaltung vor allem durch die zahlreichen Projekte und Vorhaben, die unter diesem Titel geplant und realisiert werden. Dies betrifft allem voran das persönliche Serviceportal der Stadt Zürich **«Mein Konto»**, über das Privatpersonen und zukünftig wohl auch Unternehmen städtische Dienstleistungen beziehen oder Verwaltungsgeschäfte mit der Stadtverwaltung abwickeln können.

Zu den über «Mein Konto» angebotenen **Online-Diensten** gehören insbesondere Anmeldungen, Gesuche, Bestellungen oder Terminvereinbarungen. Für solche Prozesse müssen immer auch persönliche Daten der Kundinnen und Kunden erhoben und bearbeitet werden. Die Transformation ins digitale Zeitalter ist ein idealer Zeitpunkt, bisherige Geschäftsprozesse und damit verbundene Datenbearbeitungen kritisch zu hinterfragen. Dazu gehört insbesondere die Prüfung der Verhältnismässigkeit, also der Frage, ob nur diejenigen Daten bearbeitet werden, welche für die Erfüllung der öffentlichen Aufgabe effektiv notwendig sind.

Persönliche Daten müssen geschützt werden. Dies betrifft einerseits die **Inhaltsdaten,** also alle Informationen, die beispielsweise eine Anmeldung oder ein Gesuch beinhalten. Dazu gehört auch die Kommunikation, die sich die Bevölkerung vermehrt elektronisch mit der Stadtverwaltung wünscht. Entsprechende Nachrichten oder Mitteilungen können vertrauliche Informationen enthalten, weshalb deren Übertragung geschützt werden muss. Herkömmliche E-Mail-Kommunikation erfolgt unverschlüsselt und ist deshalb für den Austausch von personenbezogenen Daten nicht ausreichend sicher. «Mein Konto» behebt dieses Defizit und bietet für elektronische Mitteilungen einen sicheren Kommunikationskanal. Geschützt werden müssen andererseits auch sogenannte **Rand- oder Verkehrsdaten.** Darunter sind Informationen über die Nutzung elektronischer Infrastrukturen zu verstehen, die in der Regel zur Gewährleistung der Funktionalität und Nachvollziehbarkeit erhoben werden. Mit der Digitalisierung gewinnen Rand- oder Verkehrsdaten auch aus datenschutzrechtlicher Optik zunehmend an Bedeutung, da auch sie unter Umständen Aussagen oder Auswertungen über Personen ermöglichen.

Die Online-Dienste, die über das Serviceportal «Mein Konto» angeboten werden, haben wie alle städtischen Vorhaben mit Informationsbearbeitungen den **städtischen ISDS-Prozess** zu durchlaufen (vgl. Grundlagen **Seite 9**). Beinhalten sie besondere Risiken für die Grundrechte der Kundinnen und Kunden, sind sie der Datenschutzstelle zur Vorabkontrolle zu unterbreiten (vgl. Fokus Datenschutz-Folgenabschätzung **Seite 52**).

«Mein Konto» und E-Government der Stadt Zürich sind Gegenstand des Interviews mit Michael Keller, Abteilungsleiter E-Government & Digitale Prozesse bei Organisation und Informatik Zürich (OIZ) (ab **Seite 73**).

«Mein Konto»-Login mit «Zürich Access»-App

Im Berichtsjahr lancierte Organisation und Informatik Zürich (OIZ) die Smartphone-App «Zürich Access», welche ein **sicheres und nutzerfreundliches Login** zu «Mein Konto» ermöglicht.

Nach einer einmaligen Registrierung und Verifizierung des eigenen Smartphones kann die «Zürich Access»-App für den vereinfachten Loginprozess verwendet werden. Bei jedem Login über die App werden die auf dem registrierten Smartphone hinterlegten **biometrischen Daten** – wahlweise Fingerabdruck oder Gesichtserkennung – genutzt, um eine sogenannte 2-Faktor-Authentifizierung sicherzustellen. Mit diesem Login-Verfahren wird nicht nur die Sicherheit, sondern gleichzeitig auch die sogenannte Usability erhöht, da die Nutzerinnen und Nutzer der App keine zusätzlichen Login-Verfahren für sensible «Mein Konto»-Services durchführen müssen.

Die Prüfung durch die Datenschutzstelle zeigte, dass die «Zürich Access»-App dem neusten technischen Stand entspricht. Die biometrischen Daten der App-Nutzenden sind ausschliesslich auf deren Smartphones abgelegt. Weder die Stadt Zürich noch die App-Entwicklerin haben den Bedarf oder die Möglichkeit, über die App auf diese Daten zuzugreifen oder sie zu anderen als den erwähnten Login-Zwecken zu verwenden.

«Steuern verwalten»

Im Berichtsjahr begleitete die Datenschutzstelle das Projekt «Steuern verwalten» bis zu seinem Go-Live auf «Mein Konto». Dabei wurde eine umfassende Prüfung durchgeführt, damit die Einwohnerinnen und Einwohner der Stadt Zürich diesem Service auch aus datenschutzrechtlicher Sicht vertrauen können.

Steuergeschäfte sind in der Stadt Zürich eines der Massengeschäfte schlechthin. Das Steueramt veranlagt jährlich ungefähr 180 000 natürliche Personen. Mit dem Service «Steuern verwalten» hat die Stadt via «Mein Konto» einen digitalen Zugang zum Steueramt geschaffen. «Steuern verwalten» erlaubt es den Zürcherinnen und Zürchern, eine Übersicht über ihre eigene Steuersituation zu gewinnen, Steuerrechnungen zu bezahlen sowie Ratenzahlungen einzurichten.

Ebenso wichtig wie diese Funktionalitäten ist die Gewährleistung, dass das Steueramt und die Steuerpflichtigen mittels «Steuern verwalten» **sicher miteinander kommunizieren** können. Wie bereits im voranstehenden Fokustext erwähnt, bietet «Mein Konto» dafür eine Lösung, welche datenschutzrechtlichen Ansprüchen entspricht.

Weiter waren aus datenschutzrechtlicher Sicht insbesondere die Themen Transparenz gegenüber den Nutzerinnen und Nutzern sowie Authentifizierung von Relevanz. Das Thema **Transparenz** gegenüber den Nutzerinnen und Nutzern beschlug in erster Linie die adressatengerechte Formulierung der Nutzungsbedingungen für den Service «Steuern verwalten». Wie jeder Service in «Mein Konto» wird auch der Zugang zu «Steuern verwalten» entsprechend der Sensibilität der darin enthaltenen Daten geschützt. Für «Steuern verwalten» musste deshalb eine **2-Faktor-Authentifizierung** implementiert werden.

Nicht primär eine datenschutz-, sondern vielmehr eine steuerrechtliche Frage betraf die rechtliche **Verbindlichkeit** des Service «Steuern verwalten». Die Datenschutzstelle regte die Klärung dieser Frage insbesondere deshalb an, weil je nach steuerrechtlicher Anforderung (beispielsweise betreffend Nachvollziehbarkeit) auch die Anforderungen an die Datenbearbeitung anders gestellt werden müssen. Die Abklärung ergab, dass das Steueramt via «Steuern verwalten» keine rechtlich verbindlichen Handlungen vornimmt. Sämtliche rechtlich verbindlichen Handlungen des Steueramts (wie die Zustellung von Rechnungen oder Verfügungen) werden den steuerpflichtigen Personen weiterhin auf dem Postweg zugestellt.

Personalbereich

Das Datenschutzrecht und das Arbeits- oder Personalrecht haben viele Gemeinsamkeiten. Das kommt nicht von ungefähr, denn für beide Rechtsgebiete ist der **Schutz der Persönlichkeit** ein wichtiges und zentrales Anliegen. Rechte und Pflichten zum Schutz der Persönlichkeit ergeben sich deshalb oft gleichzeitig aus dem Arbeits- und dem Datenschutzrecht. Für das Personalrecht der Stadt Zürich gilt dies in besonderem Masse, da es **zahlreiche Grundsätze und Prinzipien,** die bereits aufgrund des allgemeinen Datenschutzrechts gelten, nochmals ausdrücklich erwähnt: Beispielsweise das Verhältnismässigkeitsprinzip, wonach nur notwendige und geeignete Daten bearbeitet werden dürfen, das Erfordernis der genügenden Legitimation für Datenbekanntgaben oder das Einsichtsrecht in das eigene Personaldossier.

Die starke Technologisierung zahlreicher Arbeitsplätze bringt mit sich, dass mit dem Einsatz moderner Arbeitsgeräte das Verhalten oder die Leistung der Angestellten überwacht oder ausgewertet werden könnten. Nebst Fragen nach Zulässigkeit und Verhältnismässigkeit allfälliger Überwachungen oder Auswertungen am Arbeitsplatz sind es vor allem auch die **Transparenz- und Informationsmassnahmen** gegenüber den Angestellten, die Gegenstand datenschutzrechtlicher Prüfungen sein können. Die Stadt Zürich hat mit dem Erlass des städtischen Reglements über die Nutzung elektronischer Infrastrukturen oder Dienste der Stadt Zürich (REID) frühzeitig die diesbezüglich wichtigsten Grundlagen geschaffen. Bedeutung und Nutzen dieses Reglements zeigt sich auch darin, dass seither nur noch selten diesbezügliche Anfragen oder Reklamationen von städtischen Mitarbeitenden bei der Datenschutzstelle eingehen.

In personalrechtlichen Verhältnissen müssen oft auch sehr vertrauliche und sensitive **Gesundheitsdaten** bearbeitet werden, so beispielsweise im Case Management oder bei vertrauensärztlichen Abklärungen. Auch solche Belange können Anlass für Anfragen bei der Datenschutzstelle sein.

Persönlichkeitsanalyse im Personalwesen

Im Bereich der Personalrekrutierung, aber auch allgemein im Personalwesen, werden Instrumente eingesetzt, welche es HR-Verantwortlichen ermöglichen, von Bewerbenden oder Mitarbeitenden sogenannte Persönlichkeitsanalysen zu erstellen. Diese Analysen sollen beispielsweise das **Arbeits-, Sozial- oder Führungsverhalten** einer Person aufzeigen und dabei Hinweise liefern, ob eine Person spezifische Anforderungen für eine bestimmte Funktion mitbringt. Es liegt auf der Hand, dass durch solche Analysen, welche sich vertieft mit der Persönlichkeit einer betroffenen Person auseinandersetzen, eine umfangreiche und sehr sensible Datenbearbeitung vorgenommen wird. Im Berichtsjahr kontrollierte die Datenschutzstelle entsprechend eingehend den Einsatz eines solchen Persönlichkeitsanalysetools in einer Dienstabteilung.

In der städtischen Verwaltung sind Persönlichkeitsanalysen oder sogenannte Assessments bei der **Rekrutierung** von Personal verbreitet. Das zu prüfende Persönlichkeitsanalysetool sollte nicht nur bei der Rekrutierung von Personal, sondern auch bei der **Nachfolgeplanung** sowie der **Evaluation von Entwicklungsmöglichkeiten** für Mitarbeitende eingesetzt werden. Die Möglichkeit eines solch breiten Einsatzes des Tools auf verschiedene «Kategorien» von Personen, nämlich Stellenbewerbende sowie Mitarbeitende ohne konkrete Absicht für einen Stellenwechsel, warf die Frage auf, inwiefern eine Persönlichkeitsanalyse bei Mitarbeitenden der Stadtverwaltung mit dem Personalrecht vereinbar ist.

Die rechtliche Klärung hat ergeben, dass das **Personalrecht der Stadt Zürich** nur im Bewerbungsprozess eine Grundlage für den Einsatz von Persönlichkeitsanalysen bietet. Unter diesen Bewerbungsprozess fallen auch Mitarbeitende, die sich innerhalb der Verwaltung beruflich neu orientieren oder versetzen lassen möchten. Keine Grundlage findet sich im Personalrecht hingegen für den Einsatz von Persönlichkeitsanalysen bei Nachfolgeplanung oder Entwicklungsmassnahmen von Mitarbeitenden. Daraus ist zu schliessen, dass solche Eignungsprüfungen **ausserhalb des Bewerbungsprozesses grundsätzlich nicht vorgesehen** sind.

Nicht nur eine gesetzliche Grundlage, sondern auch eine gültig erteilte **Einwilligung** könnten die Verwaltung dazu ermächtigen, Persönlichkeitsanalysen durchzuführen. Dies setzt jedoch voraus, dass die Einwilligung freiwillig erfolgt. **Freiwilligkeit** ist dann zu bejahen, wenn die Einwilligung nicht in einer Zwangslage oder unter Druck getroffen wurde. Mitarbeitende müssen eine Bearbeitung ihrer Daten ohne Befürchtung von Sanktionen verweigern dürfen oder eine zuvor erteilte Einwilligung folgenlos widerrufen können. Genau hier bestehen aber im Arbeitsverhältnis Zweifel, da aufgrund der zwischen den Parteien bestehenden unterschiedlichen Machtstruktur den Angestellten häufig keine (gefühlte) andere Wahl bleibt, als einer geplanten Datenbearbeitung zuzustimmen. Im Arbeitsverhältnis stellt deshalb die Einwilligung meist eine zweifelhafte Grundlage dar.

Die betroffene Dienstabteilung hat sich aufgrund der erfolgten Abklärungen dazu entschieden, Persönlichkeitsanalysen nur in Bewerbungsprozessen durchzuführen und auf einen weiteren Einsatz dieses Tools vorerst zu verzichten. Sollte sich in Zukunft ergeben, dass Persönlichkeitsanalysen auch ausserhalb des Bewerbungsprozesses durchgeführt werden sollen, ist das städtische Personalrecht entsprechend zu ergänzen.

Betriebliches Gesundheitsmanagement

Das städtische Personalrecht verlangt von der Stadt Zürich als Arbeitgeberin, dass sie die **Gesundheit der Angestellten** schützt und fördert. Um dies sicherzustellen, setzen städtische Verwaltungsstellen zunehmend auf Prozesse und Instrumente, die in ihrer Gesamtheit betriebliches Gesundheitsmanagement genannt werden. Ziel dabei ist es, Ausfälle und Absenzen zu minimieren, Fälle des Case Managements zu verhindern und die physische und psychische Gesundheit der Mitarbeitenden zu fördern.

Im Berichtsjahr wurde die Datenschutzstelle erstmals in ein Projekt zum betrieblichen Gesundheitsmanagement miteinbezogen. Gegenstand dieses Projekts war noch nicht ein ganzheitliches Gesundheitsmanagement, sondern erst einmal nur der Teilbereich der **Früherkennung.** Zentrales Element dabei ist der **regelmässige Austausch** zwischen Vorgesetzten und Angestellten. Er findet eingebettet im Arbeitsalltag, nach Abwesenheiten jedwelcher Art, bei Verhaltens- und Leistungsveränderungen sowie vermehrten Absenzen statt. Die Gespräche haben das Ziel, mögliche Zusammenhänge zwischen vorhandenen Ressourcen und Belastungen am Arbeitsplatz zu eruieren, Unterstützungsmassnahmen zu definieren und die Wirkung der Massnahmen zu überprüfen. Die im Gespräch gemeinsam getroffenen Massnahmen werden protokolliert, auch um sie an weiteren Gesprächen überprüfen zu können. Die Früherkennung basiert auf **Freiwilligkeit.** Betroffenen Angestellten ist es somit freigestellt, ob sie dieses Angebot in Anspruch nehmen wollen oder nicht.

Im Rahmen der Früherkennung geben Mitarbeitende zum Teil sensible Informationen über sich preis. Damit sie darauf vertrauen können, dass mit ihren Personendaten korrekt umgegangen wird, müssen sie ausführlich und verständlich über die Früherkennung, deren Zielsetzung sowie die damit einhergehenden Datenbearbeitungen und Massnahmen **informiert** werden. Auf Empfehlung der Datenschutzstelle wurde hierfür ein Kommunikationskonzept erstellt, um die erforderliche Transparenz zu gewährleisten. Bei der datenschutzrechtlichen Beratung und Prüfung wurde besonderes Augenmerk auch auf eine **sachgerechte Protokollierung** gelegt. Im Rahmen der Früherkennung werden die zwischen Angestellten und Vorgesetzten besprochenen Massnahmen mittels Gesprächsprotokoll festgehalten. Protokollierungen von Mitarbeitendengesprächen sind an sich nichts Aussergewöhnliches. Mit Blick auf den Persönlichkeitsschutz der betroffenen Mitarbeitenden ist im vorliegenden Kontext aber zu berücksichtigen, dass solche Protokollierungen das **Risiko einer Stigmatisierung** mit sich bringen können. Um dieser Problematik entgegenzuwirken, werden die Protokolle losgelöst vom Personaldossier aufbewahrt und nach zwei Jahren automatisch gelöscht. Dadurch kann verhindert werden, dass sensible Informationen, die Angestellte im Rahmen der Früherkennung freiwillig erteilt haben, ins Personaldossier gelangen und sich dadurch auf sie nachteilig auswirken können.

Betriebliches Gesundheitsmanagement bringt wie erwähnt mit sich, dass die Arbeitgeberin sensible Informationen und Angaben über die Angestellten erhebt und auswertet. Für derartige Datenbearbeitungen verlangt das Datenschutzrecht **«hinreichend bestimmte» gesetzliche Regelungen.** Bearbeitet die Verwaltung sensible Personendaten, wird somit verlangt, dass sich die Rechtsgrundlagen zu den wichtigsten Modalitäten wie insbesondere benötigte Daten(kategorien) oder Verwendungszwecke präzise und verständlich äussern. In Bezug auf Informationen und Daten zur Gesundheit von Angestellten bleibt das städtische Personalrecht aber bloss allgemein und abstrakt. Es verlangt zwar von der Arbeitgeberin, dass sie auf die Gesundheit der Angestellten gebührend Rücksicht nimmt und hierfür die erforderlichen Massnahmen trifft, beinhaltet dazu aber kaum weitergehende Konkretisie-

rungen. Fehlende klare und präzise gesetzliche Grundlagen können insbesondere im Arbeitsbereich nicht einfach durch **Einwilligungen** ersetzt werden, da für Angestellte regelmässig eine Abhängigkeit gegenüber ihren Vorgesetzten besteht. Die Freiwilligkeit von Massnahmen kann deshalb grundsätzlich nur mit Zurückhaltung die Erhebung oder Auswertung von Daten durch Vorgesetzte rechtfertigen.

Für jede Massnahme des betrieblichen Gesundheitsmanagements, die zur Erhebung oder Auswertung sensibler Informationen oder Angaben über Mitarbeitende führt, müssen die jeweils erforderlichen rechtlichen Grundlagen im städtischen Personalrecht geprüft werden. Ein Abstützen beziehungsweise ein Verweis auf die Freiwilligkeit für die Angestellten rechtfertigte sich im vorliegend beurteilten Vorhaben der Früherkennung, kann sich aber bei weiteren Massnahmen für das betriebliche Gesundheitsmanagement rasch als nicht mehr ausreichend erweisen. Die Stadt Zürich als Arbeitgeberin hat bei der Einführung des Case Managements bewiesen, dass erforderliche gesetzliche Regelungen rechtzeitig geprüft und in datenschutzkonformer und praktikabler Weise erlassen werden können. Die Datenschutzstelle wies die zuständigen Verwaltungsstellen auch mit Blick auf das betriebliche Gesundheitsmanagement, das quasi als Vorstufe des Case Managements verstanden werden kann, auf die Wichtigkeit eines solchen Vorgehens hin.

Forschung, Planung und Statistik

In der Forschung, der Planung oder der Statistik werden regelmässig grosse Mengen von Personendaten bearbeitet. Im Gegensatz zu anderen Datenbearbeitungen wird hier aber nicht das Ziel verfolgt, Aussagen über einzelne Personen zu ermöglichen. Im Gegenteil: Am Schluss sollen Auswertungen und Ergebnisse vorliegen, die gerade keine solchen Aussagen mehr zulassen. Das Datenschutzrecht spricht bei solchen Konstellationen von **Datenbearbeitungen zu «nicht personenbezogenen Zwecken».** Für solche Datenbearbeitungen gelten erleichterte rechtliche Voraussetzungen, da das Risiko von Persönlichkeitsverletzungen als klein(er) erachtet wird.

Die Stadtverwaltung ist grundsätzlich berechtigt, ihre Daten auch zu Forschungs-, Planungs- oder Statistikzwecken selber zu nutzen oder öffentlichen und privaten Stellen und Instituten ausserhalb der Stadtverwaltung bekannt zu geben. Das sonst im Datenschutzrecht geltende Zweckbindungsprinzip, welches verlangt, dass Daten nur zu dem Zweck bearbeitet werden dürfen, zu welchem sie ursprünglich erhoben worden sind, findet bei Datenbearbeitungen zu nicht personenbezogenen Zwecken in der Regel keine Anwendung. Die Stadtverwaltung muss aber sicherstellen, dass Personendaten so schnell wie möglich anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind. In der praktischen Umsetzung erweist sich vor allem die **Anonymisierung** der Daten als Herausforderung. Von anonymisierten Daten wird dann gesprochen, wenn die personenbezogenen Angaben oder Merkmale vollständig entfernt sind und kein Rückschluss auf Personen mehr möglich ist.

Bei der Anonymisierung ist zu unterscheiden, ob es die sogenannten Rohdaten oder die Auswertungen betrifft. **Rohdaten** sind diejenigen Daten, die Grundlage für die Auswertungen bilden. Diese Daten können unter Umständen erst nach längerer Zeit anonymisiert werden, ansonsten das beabsichtigte Ziel der jeweiligen Forschung oder Statistik, beispielsweise bei Langzeitstudien, nicht erreicht werden könnte. Rohdaten müssen daher mit anderen Massnahmen wie beispielsweise strengen Zugriffsregeln geschützt werden. Davon zu unterscheiden sind die **Auswertungen,** also die Ergebnisse aus den jeweiligen Forschungs-, Planungs- und Statistikvorhaben. Solche Auswertungen müssen vollständig anonymisiert sein. Hier sind hohe Anforderungen an die Anonymisierung zu verlangen, da Auswertungen regelmässig auch veröffentlicht werden und da die technologischen Entwicklungen laufend weitergehende Analysen und Verknüpfungen von Daten ermöglichen.

Es kann vorkommen, dass die Stadtverwaltung für Forschungen oder Planungen nicht bereits über die dazu erforderlichen Daten verfügt und diese durch Umfragen erst noch erheben muss. Für derartige **Direkterhebungen** braucht sie eine gesetzliche Berechtigung, was sich in der Regel durch einen entsprechenden gesetzlichen Auftrag ergibt. Privatpersonen sind in der Regel nicht verpflichtet, an solchen Direkterhebungen der Stadtverwaltung mitzumachen. Die **freiwillige Teilnahme** muss bei Umfragen jeweils klar zum Ausdruck gebracht werden.

Im **Bereich der medizinischen Forschung** gelten strengere Vorschriften, vor allem in Bezug auf Aufklärungs- und Informationspflichten. Auch bereits vorhandene Daten von Patientinnen und Patienten dürfen grundsätzlich nur mit deren Einverständnis zu Forschungszwecken weiterverwendet werden.

Mikromobilitätsmanagement

Die Mobilität mit Kleinfahrzeugen (sogenannte Mikromobilität) hat in den letzten Jahren die Städte verändert. Anbieter von Leihfahrzeugen haben die Stadt Zürich geradezu geflutet, insbesondere mit E-Trottinets und Fahrrädern mit oder ohne Elektroantrieb. Da diese Fahrzeuge nach dem Prinzip «free floating» ohne fixe Station zur Verfügung gestellt werden, können sie unter Einhaltung der Parkierungsregeln irgendwo im öffentlichen Raum abgestellt werden. Dies führte zum Teil zu massiven Übernutzungen des öffentlichen Raums. Der Stadtrat hat auf diese Entwicklung reagiert: Das stationslose Anbieten von Kleinfahrzeugen im öffentlichen Raum wurde in der städtischen Benutzungsordnung geregelt und einer Bewilligungspflicht unterstellt. Die Bewilligungen können mit Auflagen verbunden werden.

Mit der Nutzung von Leihfahrzeugen fallen viele, zum Teil persönliche Daten an: Einerseits erfolgt das Ausleihen der Fahrzeuge über eine entsprechende App, welche eine **Registrierung** mit persönlichen Angaben verlangt. Andererseits verfügen die Leihfahrzeuge über GPS-Tracker, welche **Standort- und Bewegungsdaten** festhalten. Den Anbietern ist in Echtzeit bekannt, wer gerade mit welchem Fahrzeug unterwegs ist und an welchen Standorten die Leihfahrzeuge abgestellt werden und damit für andere Nutzende wieder verfügbar sind. Den Anbietern von Leihfahrzeugen stehen damit auch Personendaten zur Verfügung. Wie die Anbieter mit diesen umzugehen haben, fällt – da sie als private Unternehmen handeln – in den **Geltungsbereich des Bundesdatenschutzrechts** und damit in den Zuständigkeitsbereich des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. Auch die Stadtverwaltung ist an den Standort- und Bewegungsdaten interessiert. Einerseits sollen anhand der Daten die Bewilligungsauflagen kontrolliert und andererseits anhand von Auswertungen wichtige Erkenntnisse für die Mobilitätsplanung und Unfallforschung gewonnen werden. Für diese Zwecke nicht notwendig sind persönliche Angaben der Nutzenden. Gestützt auf die städtische Benutzungsordnung wurden die Anbieter von Leihfahrzeugen im Rahmen

von Auflagen zur Lieferung von unpersönlichen, statistischen Daten verpflichtet. Die Bekanntgabe dieser Daten an und deren Nutzung durch die Stadtverwaltung fällt in den **Geltungsbereich des kantonalen Datenschutzgesetzes IDG** und damit aufsichtsrechtlich in die Zuständigkeit der städtischen Datenschutzstelle.

Die Stadtverwaltung lässt für ihre Kontroll- und Planungsbedürfnisse Standort- und Bewegungsdaten im Rahmen eines Pilotprojekts auf einer externen (Mobilitäts-)Datenplattform speichern und auswerten. Dies erfolgt zwar mit der Identifikationsnummer der Fahrzeuge, jedoch ohne Angaben zu den registrierten Nutzenden. Aus Optik Datenschutz unproblematisch sind **Standortdaten** derjenigen Fahrzeuge, welche nicht ausgeliehen sind. Diese stehen ohne Bezug zu einer Nutzerin oder einem Nutzer und geben nur wieder, dass ein Fahrzeug an einem bestimmten Standort parkiert ist. Das Bundesamt für Energie veröffentlicht schweizweit die aktuellen Standortdaten verfügbarer Leihfahrzeuge (**www.sharedmobility.ch**). Heikel dagegen sind **Bewegungsdaten:** Auch wenn die jeweiligen Nutzerinnen oder Nutzer der Stadtverwaltung nicht namentlich bekannt sind, könnten mit diesen Daten Bewegungsmuster generiert werden, welche unter Umständen Rückschlüsse auf Einzelpersonen zulassen. Solche Daten sind daher der Stadtverwaltung zu Planungszwecken nur **in aggregierter Form** zur Verfügung zu stellen. Die Datenschutzstelle hat verlangt, dass diese Anforderung vertraglich sichergestellt wird und hat gleichzeitig mit der für das Vorhaben zuständigen Dienstabteilung geprüft, welche weiteren Datenschutzthemen mit den Anbietern der Leihfahrzeuge und dem Betreiber der Mobilitäts-Datenplattform vertraglich zu regeln sind. Mit den in der Zwischenzeit abgeschlossenen Vereinbarungen wird insbesondere sichergestellt, dass die von den Anbietern von Leihfahrzeugen der Stadtverwaltung zur Verfügung gestellten Daten vertraulich behandelt und im Rahmen des städtischen Auftrages und damit zu den obgenannten Kontroll-, und Planungszwecken sowie zur Unfallforschung bearbeitet werden.

Durchmischung an städtischen Schulen

Eine universitäre Forschungsstudie stellte vor einigen Jahren fest, dass in der Stadt Zürich die Bildungschancen der Kinder auch davon abhängen, welchem Schulhaus diese zugeteilt werden und dass damit aufgrund der Wohnsituation zum Teil ungleiche Bildungschancen bestehen. In dieser Studie wurde mit Hilfe eines Algorithmus ein datengestütztes Zuteilungsverfahren entwickelt, welches Vorschläge für eine Optimierung der Einzugsgebiete der Schulen ermöglichen und zu einer ausgewogeneren Durchmischung der Schulen beitragen soll. Die Studie hatte mediale Aufmerksamkeit erlangt und zu einer politischen Anfrage im Kantonsrat geführt.

Im Berichtsjahr prüfte die Datenschutzstelle nun eine Folgestudie, welche in Kooperation mit zwei interessierten Kreisschulbehörden die Verfeinerung der ersten Studie und insbesondere die Verbesserung des **Algorithmus** zum Ziel hatte. Von Anfang an war klar, dass der Algorithmus den zuständigen Behörden nur als Entscheidungshilfe dienen soll und damit die Schulzuteilung nach wie vor von diesen in «Handarbeit» vorgenommen wird. Das Datenschutzrecht verlangt, dass Bearbeitungen von Personendaten **transparent und nachvollziehbar** sind. Diese Anforderung gilt in erhöhtem Masse, wenn Algorithmen zur Bearbeitung solcher Daten eingesetzt werden. Erst wenn die konkrete Funktionsweise bekannt ist, kann letztlich eine datenschutzrechtliche Beurteilung vorgenommen werden. Da im Rahmen dieser Folgestudie auch sensible Informationen über die Kinder, wie beispielsweise über deren Leistungsfähigkeit oder sozialen Kompetenzen, bearbeitet wurden, verlangte die Datenschutzstelle vom Schul- und Sportdepartement ein Datenschutzkonzept, in welchem – neben weiteren Themen – insbesondere die Funktionsweise des Algorithmus detailliert und nachvollziehbar zu dokumentieren war.

Im Rahmen der Erarbeitung dieses Konzepts wurden durch das Schul- und Sportdepartement unter anderem diverse Rechtsfragen in Zusammenhang mit Schul- und Klassenzuteilungen sowie die Verhältnismässigkeit der dem Algorithmus zu Grunde gelegten Daten geklärt. Die **Zuteilungskriterien,** die für eine ausgewogene Durchmischung relevant sind, ergeben sich aus der kantonalen Volksschulverordnung sowie dem städtischen Zuteilungsreglement. Massgebend sind primär die soziale und sprachliche Herkunft und die Leistungsfähigkeit der Schülerinnen und Schüler. Ausgehend von diesen rechtlichen Vorgaben haben die Abklärungen dazu geführt, dass auf verschiedene Daten, welche anfänglich zum Aufbau des Algorithmus beantragt wurden, verzichtet werden konnte.

Der Algorithmus berücksichtigt die erwähnten Zuteilungskriterien, teilt jedoch einem Schulhaus nicht einzelne Schülerinnen und Schüler zu, sondern **«Kleinquartiere»,** in denen die Schülerinnen und Schüler wohnen. «Kleinquartiere» sind kleinräumige Einteilungen des Stadtgebiets, wie sie vom Amt für Städtebau definiert und auch von Statistik Stadt Zürich verwendet werden (im Berichtsjahr gab es 5514 solcher «Kleinquartiere»). Der Algorithmus wertet aus, in welchen Kleinquartieren Schülerinnen und Schüler mit guten oder mit schlechten Bildungschancen wohnen. Aufgrund der Kleinräumigkeit der Auswertungen können Rückschlüsse auf Einzelpersonen nicht ganz ausgeschlossen werden. Sofern die Auswertungen nur intern im Rahmen der Forschungsstudie und damit für die Optimierung der Schulzuteilung verwendet werden, ist dies – gestützt auf die erwähnten Rechtsgrundlagen – datenschutzrechtlich unproblematisch.

Problematisch und nur unter bestimmten Voraussetzungen zulässig wäre allerdings die Veröffentlichung solch **kleinräumiger Auswertungen.** Dies auch aus Gründen des Datenschutzes, aber nicht nur. Das Datenschutzrecht verlangt generell bei der Veröffentlichung von Auswertungen im Bereich Forschung, Planung und Statistik, dass aus diesen keine Rückschlüsse auf Einzelpersonen möglich sind. Dies einzuhalten, ist bei kleinräumen Auswertungen oft schwierig und erfordert eine eingehende Prüfung. Zusätzlich zum Datenschutz setzt das in der Bundesverfassung (ebenfalls)

als Grundrecht verankerte **Diskriminierungsverbot** bei der Veröffentlichung von kleinräumigen Auswertungen eine weitere Schranke. Dieses verbietet insbesondere Diskriminierungen wegen der Herkunft, der Sprache oder der sozialen Stellung. Bei Veröffentlichungen von kleinräumigen Auswertungen kann – selbst wenn diese datenschutzkonform erfolgen – das Risiko bestehen, dass es zu stigmatisierenden Kategorisierungen oder Zuordnungen kommen kann und betroffene Bewohnerinnen und Bewohner dadurch diskriminiert werden. Kleinräumige Auswertungen sind daher vor einer allfälligen Veröffentlichung auch unter diesem Aspekt genau zu prüfen.

Videoüberwachung

Videoüberwachung durch die Stadtverwaltung

Die Stadt Zürich hat für Videoüberwachung der städtischen Verwaltungsstellen eigene gesetzliche Regelungen in der **städtischen Datenschutzverordnung** erlassen. Diese Verordnung sieht vor, dass die Stadtverwaltung bei erheblichen Gefahrensituationen Videoüberwachung einsetzen darf. Erfolgt eine Videoüberwachung mit Aufzeichnungen, muss die Dienstabteilung ein **Videoreglement** erlassen und dieses der Datenschutzstelle zur Prüfung vorlegen. Betrifft die Videoüberwachung der städtischen Verwaltungsstelle öffentlichen oder allgemein zugänglichen Raum, ist das Videoreglement amtlich zu publizieren und in die **Amtliche Sammlung** der Stadt Zürich aufzunehmen.

Eine Spezialregelung gibt es für die Videoüberwachung bei **Schulgebäuden und Schulanlagen.** Hierfür hat der Stadtrat bereits vor Inkrafttreten der städtischen Datenschutzverordnung eigene Vorschriften erlassen. Die Videoüberwachung bei Schulgebäuden und Schulanlagen dient dem Schutz der Gebäude und Anlagen und beschränkt sich auf Aussenfassaden, Eingangsbereiche sowie abschliessbares Gelände wie beispielsweise Sport- oder Freizeitanlagen.

Für gewisse Verwaltungsbereiche bestehen **gesetzliche Bestimmungen zu Videoüberwachungen auf Bundes- oder Kantonsebene,** so vor allem für den öffentlichen Verkehr und die Polizei. Im Geltungsbereich dieser Bestimmungen kommen die städtischen Regelungen nicht zur Anwendung.

Videoüberwachung durch Private

Für Videoüberwachung durch Private sind die privatrechtlichen Bestimmungen des **Bundesgesetzes über den Datenschutz** massgebend. Daraus ergibt sich, dass für Beratung und Aufsicht bei Videoüberwachung durch Private grundsätzlich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zuständig ist.

Die Stadt Zürich hat das **Beratungsangebot** bei Videoüberwachung durch Private **erweitert**. Seit November 2020 können sich Privatpersonen bei Fragen oder Anliegen zur Videoüberwachung auch an die städtische Datenschutzstelle wenden. Voraussetzung ist, dass die fragliche Videoüberwachung öffentlichen Grund der Stadt Zürich tangiert. Die städtische Datenschutzverordnung wurde hierfür um eine entsprechende **Beratungs- und Vermittlungskompetenz der Datenschutzstelle erweitert**.

Städtische Videoreglemente nach Datenschutzverordnung

Beratungen und Prüfungen

Die Datenschutzverordnung der Stadt Zürich verpflichtet die Stadtverwaltung, für Videoüberwachungen mit Aufzeichnung Reglemente zu erstellen. In den zehn Jahren, seit die Datenschutzverordnung in Kraft ist, haben zahlreiche städtische Dienstabteilungen Videoreglemente erstellt. Die Datenschutzstelle hat die Dienstabteilungen dabei beraten und die jeweiligen Videoreglemente geprüft. So auch im Berichtsjahr.

Die Datenschutzstelle stellt regelmässig fest, dass die **Erarbeitung von Videoreglementen** eine **schwierige Aufgabe** darstellt und von den zuständigen Dienstabteilungen sowohl in fachlicher als auch in zeitlicher Hinsicht oft unterschätzt wird. Verlangt wird zum einen juristisches Wissen – insbesondere hinsichtlich Voraussetzungen und Anforderungen der Videoüberwachung sowie hinsichtlich Formulierung von Reglementen. Zum anderen bedarf es aber auch des technischen Know-hows über die jeweilige Videoanlage sowie der Kenntnis über die internen Prozesse und Zuständigkeiten der Dienstabteilung. Um all diesen Aspekten gerecht zu werden, sind interne Abklärungen und **interdisziplinäre Zusammenarbeit** unumgänglich. Oft müssen sich die Dienstabteilungen erst einmal ganz grundsätzlich mit dem Thema Videoüberwachung und den diversen Anforderungen auseinandersetzen, was die Datenschutzstelle im Rahmen ihrer Beratung und Prüfung regelmässig einfordert. Nebst der Einhaltung der rechtlichen Anforderungen zur Videoüberwachung legt die Datenschutzstelle stets auch grossen Wert auf Vollständigkeit und Verständlichkeit der Reglemente.

Zu den Videoreglementen städtischer Verwaltungsstellen gehen bei der Datenschutzstelle kaum je Anfragen aus der Bevölkerung ein. Auch im Berichtsjahr blieben diesbezügliche Anfragen aus.

Übersicht über städtische Videoreglemente

Aktuell haben 13 städtische Dienstabteilungen Videoüberwachungen gestützt auf die Datenschutzverordnung der Stadt Zürich im Einsatz. Es sind dies die Reglemente der Dienstabteilungen Stadtpolizei, Organisation und Informatik, Stadtspitäler Triemli und Waid, Städtische Gesundheitsdienste, Immobilien, Liegenschaften, Sportamt, Museum Rietberg, Wasserversorgung, Entsorgung + Recycling, Tiefbauamt und Elektrizitätswerk. Abrufbar sind die Reglemente in der **Amtlichen Sammlung der Stadt Zürich**.

Videoüberwachung durch Private

Für die neue Beratungs- und Vermittlungskompetenz der Datenschutzstelle wurde in der städtischen Datenschutzverordnung folgende Bestimmung eingeführt:

Bei Videoüberwachung durch Privatpersonen, die den öffentlichen oder allgemein zugänglichen Raum der Stadt tangiert, kann die oder der Datenschutzbeauftragte auf Anfrage hin:

a. Privatpersonen über das anwendbare Recht und die sich daraus ergebenden Rechte, Pflichten und Zuständigkeiten beraten;
b. zwischen betroffenen Personen oder Institutionen vermitteln.

Die Datenschutzstelle hat ihre **Webseite** auf das neue Beratungs- und Vermittlungsangebot für Private ausgerichtet. Auf der Webseite wird auf die allgemeinen Voraussetzungen für private Videoüberwachung und die besondere Problematik, wenn dabei öffentlicher Raum betroffen ist, hingewiesen. Diese Informationen sind in Frage- und Antwortform gegliedert und in gut verständlicher Sprache verfasst. Das Informationsangebot auf der Webseite soll aber nicht die eigentliche Beratung der Datenschutzstelle darstellen, sondern nur Einstieg oder Ausgangslage hierfür sein. Beratungen zu Videoüberwachung erfordern, dass die konkreten Umstände wie Ort, Ausmass, Zweck, Verantwortliche, Betroffene und dergleichen bekannt sind. Am effektivsten und gewinnbringendsten erfolgen Beratungen zu Videoüberwachung im direkten Gespräch. Die Datenschutzstelle bringt deshalb auf ihrer Webseite vor allem auch zum Ausdruck, dass sie für Beratungen und Informationen zur Videoüberwachung im öffentlichen Raum auf einfachem und direktem Weg via Telefon oder Kontaktformular erreichbar ist.

Im Berichtsjahr blieben die Beratungen der Datenschutzstelle zu Videoüberwachung durch Private mit 15 Anfragen auf tiefem Niveau.

Webcam

Eine besondere Form des Videoeinsatzes stellen die sogenannten Webcams dar, zu welchen die Datenschutzstelle im Berichtsjahr mehrere Anfragen erhielt. Wer schätzt sie nicht – die Vielzahl der im Internet abrufbaren Webcams, welche Live-Bilder von touristischen Regionen, Strassenzuständen oder schlicht dem Wetter liefern? Entsprechend ihrer Beliebtheit sind heute zahlreiche Webcams auch auf dem Gebiet der Stadt Zürich im Einsatz.

Bei einer Webcam handelt es sich um eine Videokamera, welche ihre Bilder direkt über das Internet veröffentlicht. Dieses «Live-Schalten» der Bilder über das Web ist mithin auch der grösste Unterschied zu «normaler» Videoüberwachung. Auch werden die Bilder von Webcams üblicherweise nicht aufgezeichnet.

Webcam-Bilder sind nur dann datenschutzrechtlich relevant, wenn abgebildete **Personen bestimmbar** und somit identifizierbar sind. Bestimmbar ist eine Person dann, wenn sich ihre Identität aus dem Kontext (z. B. Kleidung, Fahrzeuge etc.) oder durch Kombination mit zusätzlichem Wissen ergibt, solange dies ohne unverhältnismässigen Aufwand möglich ist. Die Frage nach der Bestimmbarkeit einer Person ist nicht immer einfach zu beantworten und muss regelmässig im Einzelfall abgeklärt werden. Ein Anwendungsbeispiel aus dem Berichtsjahr betraf die Fragestellung, ob eine Identifizierung auch anhand von Bootsplätzen, bei welchen sich Personen aufhalten (und diese nicht nur passieren), möglich sein kann. Obwohl es in der Stadt Zürich kein öffentliches Register der Bootsplätze und ihrer Halterinnen und Halter gibt, kann dennoch nicht ausgeschlossen werden, dass eine Person Kenntnis des Inhabers eines Bootsplatzes erlangt und diesen mittels Webcam beobachtet. Im Fazit kann somit eine Bestimmbarkeit einer Person durch das Anzeigen eines Bootsplatzes nicht ausgeschlossen werden.

Sind Personen auf Webcam-Bildern identifizierbar, ist das Datenschutzrecht anwendbar. Webcams dürfen dann nur unter Beachtung der datenschutzrechtlichen Grundsätze eingesetzt werden. Die wichtigste Voraussetzung ist, dass die Bildübertragungen rechtmässig erfolgen. Dazu braucht eine Betreiberin einer Webcam entweder ein **überwiegendes privates oder öffentliches Interesse,** eine gesetzliche Rechtfertigung oder die **Einwilligung** der betroffenen Personen. Da beim Einsatz von Webcams in aller Regel keine dieser Berechtigungen gegeben ist, sind Webcams aus datenschutzrechtlicher Sicht nur dann zulässig, wenn keine Personendaten erhoben werden. Sie müssen deshalb so eingestellt sein, dass keine Personen bestimmbar sind, mit anderen Worten Menschen auf den Bildern nicht identifiziert werden können. Beim erwähnten Webcam-Beispiel wurde dies dadurch sichergestellt, dass die Bildbereiche, die die Bootsplätze betreffen, nur verpixelt wiedergegeben werden.

Videobasierte Analyse- und Zählsysteme

Videoüberwachung steht regelmässig als Synonym für Beobachtung und Kontrolle von Personen und Örtlichkeiten mittels Aufzeichnung von Bildern. Videotechnologie kann heute aber weit mehr als beobachten und aufzeichnen, weshalb sie zunehmend Bestandteil komplexer technischer Systeme wird. **Intelligente Videosysteme** können mittels spezifischer Sensoren beispielsweise Geschwindigkeit, Abstand, Blick- und Laufrichtung oder sogar die Körpertemperatur von Personen **messen und analysieren** oder Personen mit Hilfe von Gesichtserkennungsfunktionen **identifizieren.** Je nach Funktionsumfang können solche Systeme tief in die Privatsphäre der Bürgerinnen und Bürger eingreifen. Die Stadtverwaltung ist deshalb verpflichtet, den Einsatz solcher Systeme jeweils einer Datenschutz-Folgenabschätzung zu unterziehen und je nach damit verbundenen Risiken der Datenschutzstelle zur Vorabkontrolle zu unterbreiten (vgl. Fokus Datenschutz-Folgenabschätzung **Seite 52**).

Bewegungsanalysen in Spitälern

Sich in einem Spital als Besucherin oder Besucher zurecht zu finden, ist oft nicht einfach. Die erste wichtige **Steuerung der Besucherströme** erfolgt im Eingangsbereich. Eine optimale Gestaltung dieses Bereichs ist für das Funktionieren eines Spitals bedeutsam. Die Analyse der Besucherbewegungen kann wichtige Hinweise für die Planung und Gestaltung der Eingangsbereiche geben.

Die beiden Stadtspitäler testen in einem Pilotprojekt Systeme zweier Anbieter zur Optimierung der Eingangsbereiche. Dabei werden die Systeme so eingesetzt, dass die Privatsphäre der Personen gewahrt bleibt. Hierfür werden – als erste und wichtigste Voraussetzung – die **Bilddaten bereits an der Quelle vollständig anonymisiert,** damit keine Personendaten anfallen. Die beiden Testsysteme verfolgen hierfür unterschiedliche Ansätze: Das eine Testsystem wandelt Videobilder in Metadaten ohne Personenbezug um und spei-

chert nur diese Daten. Das andere System verpixelt die Videobilder und speichert nur diese Aufnahmen. Da für Analysen zu Zwecken der Raumoptimierung keine Personendaten benötigt werden, ist der Einsatz videobasierter Überwachungssysteme zu diesen Zwecken nur zu rechtfertigen, wenn auch tatsächlich keine Personendaten bearbeitet werden.

Zusätzlich zur Sicherstellung der Anonymisierung wird auch der **Funktionsumfang reduziert.** Auf hochsensible Funktionen wie beispielsweise Gesichtserkennung und Körpertemperaturmessung, welche für die räumliche Optimierung des Eingangsbereichs nicht relevant sind, wird verzichtet. Ausserdem werden die Daten einzig auf einem lokalen System gespeichert, auf welches nur ein definierter Personenkreis Zugriff hat. Die Datenschutzstelle verlangte die Ausarbeitung eines Datenschutzkonzeptes, in welchem die vorgesehenen Datenbearbeitungen beschrieben und alle zum Schutze der Privatsphäre notwendigen Massnahmen verbindlich geregelt und dokumentiert werden.

Personenzählsystem in Hallenbädern

Als Massnahme zur Eindämmung der Corona-Pandemie musste in zahlreichen Innenräumen die zulässige Personenzahl eingeschränkt werden. Davon betroffen waren auch die städtischen Hallenbäder. Um diese Anforderung möglichst ressourcenschonend zu erfüllen, führte das Sportamt im Berichtsjahr ein Personenzählsystem ein.

Das Personenzählsystem nutzt videobasierte Sensoren, welche über dem Eingang an die Decke montiert sind. Geht eine Person unter dem Sensor durch, erkennt die Videofunktion sie als menschliche Gestalt und wertet ihre Bewegungsrichtung aus. Eintritte werden mit einem «+», Austritte mit einem «–» vermerkt. Zusätzlich dazu werden die Uhrzeit und die Angabe des jeweiligen Sensors beziehungsweise des Eingangs aufgezeichnet. Die Videofunktion des Sensors speichert keine Bilder, sondern dient ausschliesslich als Grundlage für eine **Auswertung in Zahlen und Grafiken.** Die Informationen, auf die das Sportamt durch den Einsatz dieses Personenzählsystems Zugriff erhält, enthalten keine Personendaten und sind somit aus datenschutzrechtlicher Sicht unbedenklich.

Löschung und Archivierung

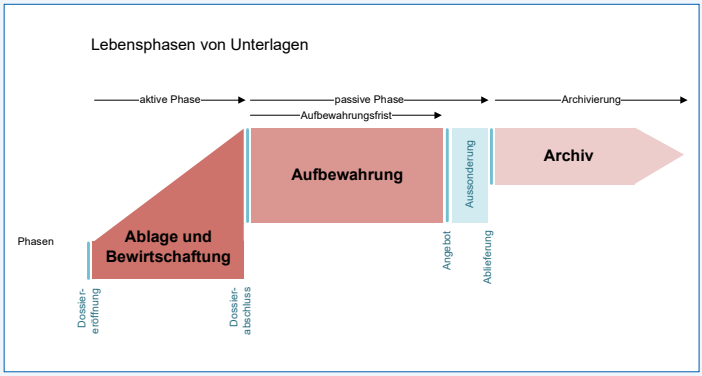
Der **Grundsatz der Verhältnismässigkeit** verlangt, dass Personendaten nur soweit bearbeitet werden, wie dies zur Erfüllung gesetzlicher Aufgaben geeignet und erforderlich ist. Aus diesem allgemeinen Bearbeitungsgrundsatz ergibt sich auch die Verpflichtung, dass Personendaten, die nicht mehr benötigt werden, gelöscht werden. Verwaltungsstellen haben somit – ausgehend von ihren jeweiligen gesetzlichen Aufgaben – zu prüfen, wann die von ihnen bearbeiteten Personendaten zu löschen sind und sie haben durch technische oder organisatorische Massnahmen sicherzustellen, dass die Löschungsfristen eingehalten werden.

Diese Verpflichtung zur Löschung steht jedoch **unter zweifachem Vorbehalt:**

– **Spezial- und Bereichsgesetzgebungen** können für spezifische Datenbearbeitungen verbindliche Löschfristen vorschreiben. So verlangt beispielsweise das kantonale Polizeigesetz, dass Aufzeichnungen technischer Überwachungsmassnahmen spätestens nach 100 Tagen zu löschen sind, soweit sie nicht für Straf-, Zivil- oder Verwaltungsverfahren benötigt werden.

– Eine Besonderheit der Verwaltung ist die sogenannte **Anbietepflicht an das Archiv.** Verwaltungsstellen haben ihre nicht mehr benötigten Informationen vor einer allfälligen Löschung dem zuständigen Archiv (im Falle der Stadt Zürich dem Stadtarchiv) zur Übernahme anzubieten. Dieses prüft die angebotenen Informationen unter dem **Gesichtspunkt der Archivwürdigkeit** und legt fest, welche vom Archiv übernommen werden.

Verwaltungsstellen dürfen gestützt auf das kantonale Informations- und Datenschutzgesetz (IDG) und das kantonale Archivrecht nicht mehr benötigte Informationen **während höchstens zehn Jahren bei sich aufbewahren.** Innerhalb dieser Frist müssen sie diese Informationen dem Archiv anbieten und – soweit nicht vom Archiv übernommen – löschen. Vorbehalten bleiben auch hier spezial- oder bereichsspezifische Vorschriften wie beispielsweise das kantonale Patientinnen- und Patientengesetz, welches Aufbewahrungsfristen von 10 bis 50 Jahren für Patientendokumentationen vorsieht.



Übersicht aus der Richtlinie «Digitale Ablieferung an das Stadtarchiv» des städtischen Records Managements.

Die fortschreitende **Digitalisierung** führt dazu, dass in der Verwaltung Informationen zunehmend (nur noch) in digitaler Form geführt und bearbeitet werden. Diese Entwicklung wirkt sich auch auf die Archivierung aus, da Informationen aus der Stadtverwaltung künftig vermehrt (nur noch) in digitaler Form an das Stadtarchiv übergeben werden. Damit auch diese Form der Archivierung sichergestellt werden kann, muss nicht nur die Löschung, sondern vermehrt auch die Archivierung frühzeitig, das heisst **bereits bei der Planung und Entwicklung** von Applikationen und Systemen, entsprechend mitberücksichtigt werden.

«KluS» – Klassen- und Schuladministration

Ein Projekt aus dem Berichtsjahr, bei dem die Löschung und Archivierung ein zentraler Prüfpunkt war, ist die Webapplikation «KluS» (Klassen- und Schuladministration). «KluS» dient der Verwaltung sämtlicher organisatorischer sowie zeugnisrelevanter Informationen und wird sowohl von Lehrpersonen als auch von Schulleitungen und Schulsekretariaten genutzt, um die Zusammenarbeit in den pädagogischen Teams zu erleichtern. Jeweils zum Semesterende werden in «KluS» die Zeugnisse, Lernberichte und Absenzenlisten erstellt und über eine Schnittstelle dem Schulamt zur Aufbewahrung in einem von «KluS» losgelösten System zugestellt.

Bei einem Projekt dieser Grössenordnung, bei dem zahlreiche Personen und Funktionen auf Daten zugreifen, war die genaue Prüfung der Zugriffs- und Berechtigungsregeln zentral. Viel weniger offensichtlich, aber nicht minder wichtig war die Bestimmung der Aufbewahrungs- und Löschfristen der in «KluS» erfassten Daten. Grundsätzlich müssen Daten immer dann gelöscht werden, sobald sie ihren Zweck erfüllt haben. Bei den Daten in «KluS» ist dies gegeben, nachdem die Zeugnisse, Lernberichte und Absenzenlisten erstellt und ausgedruckt wurden. Nun schreibt aber im vorliegenden Kontext das kantonale Reglement über die Ausstellung der Schulzeugnisse (Zeugnisreglement) vor, dass Zeugnisse, Lernberichte und Absenzenlisten in Kopie archiviert werden müssen. Diese archivwürdigen Dokumente basieren wie erwähnt auf den Informationen aus «KluS» und werden in einem weiteren System aufbewahrt, bis sie dem Archiv angeboten werden. Durch diese Verbindung drängte sich die Frage auf, inwiefern die erwähnten Archivvorschriften des Zeugnisreglements auch für die Planung und Entwicklung von «KluS» relevant und zu beachten sind. Zur Klärung dieser Frage verlangte die Datenschutzstelle beim Stadtarchiv eine Beurteilung der Archivwürdigkeit. Dabei kam das Stadtarchiv zum Schluss, dass die in Frage stehenden Daten aus «KluS» nicht archivwürdig sind.

Mit dieser Beurteilung des Stadtarchivs stand fest, dass im Projekt «KluS» keine Archivierung und damit auch keine diesbezüglichen technischen Anforderungen eingeplant werden müssen. Für das Schulamt verblieb aber die Anforderung, angemessene, auf den Zweck von «KluS» ausgerichtete Löschfristen zu definieren. Es bestimmte, dass sämtliche Daten aus «KluS» jeweils ein Semester nach dem Stufenübertritt gelöscht werden. Diese Frist stützt sich in erster Linie auf den Anspruch der individuellen, schulischen Förderung. Sowohl die Löschfrist als auch die Begründung waren für die Datenschutzstelle nachvollziehbar.

Datenschutz-Folgenabschätzung

Das kantonale Gesetz über die Information und den Datenschutz (IDG) verpflichtet Behörden und Verwaltungsstellen, bei Bearbeitungen von Personendaten die **Risiken für die Grundrechte der betroffenen Personen zu bewerten.** Das Instrument dazu heisst Datenschutz-Folgenabschätzung (§ 10 Abs. 1 IDG).

Die Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen wurde per Juni 2020 ins IDG eingeführt, da Bund und Kantone verpflichtet sind, die Anforderungen, die sich aus der Europaratskonvention 108 und der EU-Richtlinie zum Datenschutz (Richtlinie 2016/680) ergeben, in ihre Gesetzgebungen zu übernehmen (vgl. dazu TB 2019 Seite 59 ff).

Eine Datenschutz-Folgenabschätzung ist **für alle beabsichtigten Bearbeitungen von Personendaten** durchzuführen. Die Pflicht gilt nicht nur für neue, sondern auch für bereits bestehende Datenbearbeitungen, sofern sie wesentlich verändert werden. Nicht relevant ist, ob eine Bearbeitung von Personendaten als (IT-)Projekt, (IT-)Vorhaben oder dergleichen bezeichnet wird und ob oder welche Informations- und/oder Kommunikationstechnologien eingesetzt werden. Massgebend ist einzig der Umstand, dass Personendaten bearbeitet werden.

In direktem Zusammenhang mit der Datenschutz-Folgenabschätzung steht die Pflicht, wonach die **Einhaltung der Datenschutzbestimmungen sicherzustellen** ist (§ 13 Abs. 1 IDG). Auch diese Pflicht wurde per Juni 2020 ins IDG eingeführt. Durch die Datenschutz-Folgenabschätzung schaffen die Behörden und Verwaltungsstellen die Voraussetzung dafür, dass sie den Nachweis der Einhaltung der Datenschutzvorschriften erbringen können.

Zeigt eine Datenschutz-Folgenabschätzung, dass eine beabsichtigte Bearbeitung von Personendaten **besondere Risiken** für die Grundrechte der betroffenen Personen beinhaltet, so ist sie der Datenschutzstelle vorab zur Prüfung zu unterbreiten (§ 10 Abs. 2 IDG). Diese Prüfung heisst **Vorabkontrolle** und besteht seit Erlass des IDG im Jahre 2008. Mit der Vorabkontrolle prüft die Datenschutzstelle, ob eine beabsichtigte Bearbeitung von Personendaten die **rechtlichen, technischen und organisatorischen Rahmenbedingungen** einhält. Die Vorabkontrolle beinhaltet keine Detailprüfung einzelner Bearbeitungsschritte oder Massnahmen, sondern beschränkt sich auf eine Prüfung derjenigen datenschutzrechtlichen Voraussetzungen und Anforderungen, welche bei den jeweiligen Datenbearbeitungen von erhöhter Relevanz sind.

Umsetzung der Datenschutz-Folgenabschätzung

Was eine Datenschutz-Folgenabschätzung zu beinhalten hat, regelt das IDG nicht. Im Gegensatz dazu bestimmt das mittlerweile revidierte Datenschutzgesetz des Bundes (DSG), dass eine Datenschutz-Folgenabschätzung aus folgenden Elementen zu bestehen hat: Beschreibung der geplanten Bearbeitung, Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie Massnahmen zum Schutz der Persönlichkeit und der Grundrechte. Diese inhaltliche Vorgabe hat sinngemäss auch für das IDG zu gelten.

Beschreibung der beabsichtigten Bearbeitung von Personendaten

Die Datenschutz-Folgenabschätzung bringt für die Stadtverwaltung hinsichtlich Beschreibung der Datenbearbeitungen keine wesentlichen Änderungen mit sich. Behörden und Verwaltungsstellen der Stadt Zürich waren bereits bisher verpflichtet, beabsichtigte Datenbearbeitungen zu beschreiben. Im Rahmen des städtischen ISDS-Prozesses (vgl. Grundlagen **Seite 9**) erfolgt dies mit den sogenannten **ISDS-Grundlageninformationen,** welche in der Regel auch einen Projektauftrag beinhalten.

Bewertung der Risiken für die Grundrechte der betroffenen Personen

Auch eine Bewertung der Risiken erfolgte bereits bisher im Rahmen des städtischen ISDS-Prozesses. Mit der neu eingeführten Datenschutz-Folgenabschätzung haben sich die Anforderungen an die Risikobewertung jedoch erhöht. Um den Behörden und Verwaltungsstellen der Stadt Zürich für die verlangte Risikobewertung ein Instrument in die Hand zu geben, hat die Datenschutzstelle eine Vorlage für eine sogenannte **Schwellenwertanalyse** erstellt. Diese beinhaltet einen **Katalog an Gründen und Kriterien,** die Anlass geben, eine Bearbeitung von Personendaten als risikobehaftet zu bewerten. Diese Gründe und Kriterien sind in Kategorien eingeteilt und als Fragen formuliert, so beispielsweise ob

- vom Vorhaben Kinder oder Jugendliche betroffen sind,
- besondere Personendaten bearbeitet werden (z. B. Religion, Gesundheit, Biometrie, Profiling),
- Berufsgeheimnisse tangiert sind,
- eine Beobachtung, Überwachung oder systematische Kontrolle bezweckt wird,
- Technologien wie Gesichtserkennung, Künstliche Intelligenz oder Analyse-Tools eingesetzt werden.

Der Katalog ist nicht abschliessend und wird von der Datenschutzstelle den technologischen, rechtlichen und gesellschaftlichen Entwicklungen entsprechend laufend angepasst.

Logo des verantwortlichen Organs (DA/Dept)

	Ja	Nein
Werden im Rahmen des Projekts/Vorhabens Angaben oder Informationen zu städtischen Angestellten zu Bewertungs-, Beurteilungs- der Kontrollzwecken bearbeitet?	☐	☐
Berufsgeheimnis oder besondere Geheimhaltungspflichten		
Werden im Rahmen des Projekts/Vorhabens Personendaten bearbeitet, welche einem Berufsgeheimnis unterliegen?	☐	☐
Werden im Rahmen des Projekts/Vorhabens Personendaten bearbeitet, welche einer besonderen Geheimhaltungspflicht[5] unterliegen?	☐	☐
Zweck der Datenbearbeitung		
Beinhaltet das Projekt/Vorhaben Bearbeitungsvorgänge, welche die Beobachtung, Überwachung oder systematische Kontrolle von Betroffenen zum Ziele haben?	☐	☐
Sollen mit dem Projekt/Vorhaben Verfahren zur Automatisierung von personenbezogenen Einzelentscheidungen realisiert werden?	☐	☐
Werden besondere Personendaten zu *nicht personenbezogenen Zwecken* erhoben oder bekanntgegeben?[6]	☐	☐
Art der Datenbearbeitung		
Werden im Rahmen des Projekts/Vorhabens besondere Personendaten mittels eines Abrufverfahrens[7] bekannt gegeben oder zur Verfügung gestellt?	☐	☐
Beinhaltet das Projekt/Vorhaben die Erhebung oder Bearbeitung von Informationen, die Rückschlüsse auf den Standort von Personen geben können? Beispielsweise eine Lokalisierung via Mobilfunk, Bluetooth, WLAN oder GPS.	☐	☐
Werden Technologien eingesetzt, die in erhöhtem Masse Risiken für den Persönlichkeitsschutz Betroffener mit sich bringen können? Beispielsweise		☐
Gesichtserkennung	☐	
Künstliche Intelligenz	☐	
Data Mining / Analyse-Tools	☐	
Andere ……..	☐	

Auszug aus Formular Schwellenwertanalyse der Datenschutzstelle

Damit eine Bewertung von Risiken, die eine Datenbearbeitung für die Grundrechte betroffener Personen mit sich bringen kann, korrekt durchgeführt werden kann, bedarf es entsprechender Kenntnisse des Datenschutzrechts. Die Datenschutzstelle hat deshalb den städtischen Verwaltungsstellen empfohlen, die Schwellenwertanalysen durch ihre **Rechtsdienste** durchführen zu lassen oder diese hierfür mindestens beizuziehen. Im Fachintranet Datenschutz wird die Schwellenwertanalyse beschrieben und als Formular zur Verfügung gestellt.

Massnahmen zum Schutz der Grundrechte der betroffenen Personen

Wenn von Massnahmen zum Schutz von Persönlichkeit und Grundrechten die Rede ist, stehen regelmässig diejenigen Massnahmen im Vordergrund, die die Informationssicherheit gewährleisten und sich hierfür nach internationalen Standards und «Good Practices» richten. Die Stadt Zürich kennt seit 2014 das **Handbuch für Informationssicherheit,** mit welchem die technischen und organisatorischen Vorgaben verbindlich definiert werden, die erforderlich sind, um den Basisschutz der Informationen und Systeme der Stadtverwaltung zu gewährleisten.

Im Rahmen der Datenschutz-Folgenabschätzung dürfen die Massnahmen nicht auf Sicherheitsmassnahmen beschränkt bleiben. Die Datenschutz-Folgenabschätzung verlangt, dass für eine beabsichtigte Datenbearbeitung alle relevanten datenschutzrechtlichen Anforderungen und Massnahmen geprüft, bewertet und dokumentiert werden. Die Datenschutzstelle empfiehlt den städtischen Behörden und Verwaltungsstellen, diese Prüfung, Bewertung und Dokumentation anhand eines **Datenschutz-Konzepts** durchzuführen und hat hierfür ein entsprechendes **Merkblatt** erarbeitet. Inhalt eines Datenschutz-Konzepts sollen nebst den Prüfergebnissen zu den zentralen Datenschutzprinzipien (Gesetzmässigkeit, Zweckbindung, Verhältnismässigkeit, Transparenz) insbesondere auch Beurteilungen, Regelungen oder Massnahmen zu Löschung und Archivierung, Zugriffsrechten, Auskunftsrechten, Auftragsbearbeitung, Verantwortung oder verbleibenden Restrisiken sein. Das Datenschutz-Konzept nach Empfehlung der Datenschutzstelle ist in einem

generischen Sinne zu verstehen und – ausgerichtet an der konkret zu beurteilenden Datenbearbeitung – verhältnismässig und risikoadäquat umzusetzen.

Anpassung des städtischen ISDS-Prozesses

Aufgrund der jüngsten IDG-Revision, mit der die Datenschutz-Folgenabschätzung sowie die Pflicht, die Einhaltung der Datenschutzbestimmungen sicherzustellen, eingeführt wurden, haben die Fachstelle Informationssicherheit von Organisation und Informatik Stadt Zürich (OIZ) und die Datenschutzstelle den städtischen ISDS-Prozess (vgl. Grundlagen **Seite 9**) angepasst. Werden im Rahmen eines Projekts oder Vorhabens Personendaten bearbeitet, ist neu eine **Schwellenwertanalyse** durchzuführen. Ergibt diese, dass besondere Risiken für die Grundrechte betroffener Personen vorliegen, sind die datenschutzrechtlichen Anforderungen anhand eines **Datenschutz-Konzepts** zu prüfen und zu dokumentieren. Diese Neuerungen bringen mit sich, dass die **Rechtsdienste** von Behörden und Verwaltungsstellen vermehrt in Projektorganisationen oder Abläufe involviert werden, um die verlangten rechtlichen Prüfungen und Beurteilungen nicht nur fachlich, sondern auch frühzeitig sicherstellen zu können.

Weitgehend unverändert im städtischen ISDS-Prozess konnte die Prüfung der Informationssicherheit gemäss § 7 IDG und dem Handbuch Informationssicherheit der Stadt Zürich sowie der Beschrieb der erforderlichen Massnahmen bleiben. Hierfür ist ein **Informationssicherheits-Konzept** zu erstellen, das von der Fachstelle Informationssicherheit geprüft und – auch zuhanden der Datenschutzstelle – beurteilt wird.

Meldepflicht

Das kantonale Gesetz über die Information und den Datenschutz (IDG) verpflichtet Behörden und Verwaltungsstellen, bestimmte Datenschutzvorfälle der Datenschutzstelle zu melden und betroffene Personen zu informieren (§ 12a IDG). Unter Datenschutzvorfällen sind vor allem **Sicherheitsvorfälle** und **unbefugte Bearbeitungen von Personendaten** zu verstehen. Meldepflichtig sind sie, wenn die **Grundrechte betroffener Personen gefährdet** sind.

In zeitlicher Hinsicht verlangt das IDG, dass die Meldung an die Datenschutzstelle **unverzüglich** zu erfolgen hat.

Behörden und Verwaltungsstellen haben nicht nur die Datenschutzstelle, sondern auch **die betroffenen Personen zu informieren,** wenn es die Umstände erfordern oder die Datenschutzstelle dies verlangt. Von einer solchen Information kann abgesehen werden, wenn es die Umstände nicht erfordern oder wenn überwiegende öffentliche oder private Interessen entgegenstehen.

Die primären Ziele der Meldepflicht sind in der (raschen) **Schadensbegrenzung** und der **Transparenz** gegenüber Betroffenen zu sehen. Die Meldepflicht bringt gleichzeitig auch eine aufsichtsrechtliche **Rechenschaftspflicht** mit sich und stellt damit auch ein Instrument zur Einhaltung der Datenschutzbestimmungen dar.

Diese Melde- und Informationspflicht wurde per Juni 2020 ins IDG eingeführt, da Bund und Kantone verpflichtet sind, die Anforderungen, die sich aus der Europaratskonvention 108 und der EU-Richtlinie zum Datenschutz (Richtlinie 2016/680) ergeben, in ihre Gesetzgebungen zu übernehmen.

Umsetzung der Meldepflicht

Die neue Meldepflicht nach IDG wird sowohl die Stadtverwaltung als auch die Datenschutzstelle noch vor einige Herausforderungen stellen. Einerseits deshalb, weil die gesetzliche Meldepflicht wenig präzise formuliert ist und andererseits, weil die Meldepflicht rechtliche Fragen mit sich bringt, die erst noch geklärt werden müssen.

Auslegung der gesetzlichen Bestimmung (§ 12a IDG)

Zu melden sind «die unbefugte Bearbeitung oder der Verlust von Personendaten». Mit dieser Formulierung definierte der kantonale Gesetzgeber eine der beiden Grundvoraussetzungen der Meldepflicht äusserst offen und unklar. Sowohl der im IDG nicht definierte Begriff «unbefugt» als auch derjenige der «Bearbeitung», der gemäss IDG jeden Umgang mit Informationen meint, könnten dazu führen, dass an sich jeder Verstoss gegen eine datenschutzrechtliche Vorschrift als meldepflichtig bewertet werden könnte. Eine solche Auslegung entspricht jedoch nicht Sinn und Zweck der Meldepflicht.

Im Gegensatz zum IDG beschränken sowohl das eingangs erwähnte europäische Recht als auch das mittlerweile revidierte Bundesdatenschutzgesetz die meldepflichtigen Vorfälle bereits vom Wortlaut her auf «Verletzungen der Datensicherheit». Da der Grund für die Einführung einer Meldepflicht ins IDG (einzig oder mindestens primär) in der Sicherstellung der Anforderungen aus dem erwähnten europäischen Recht zu sehen ist, wird die Meinung vertreten, dass sich auch die Meldepflicht nach IDG auf Sicherheitsvorfälle zu beschränken habe. Eine solche Interpretation ist nach Ansicht der Datenschutzstelle mit dem Wortlaut von § 12a IDG nicht vereinbar und verkennt, dass es dem kantonalen Gesetzgeber freigestellt ist, über den europäischen Minimalstandard hinaus weitere Vorfälle für meldepflichtig zu bestimmen.

Die Datenschutzstelle vertritt die Ansicht, dass die Meldepflicht nach IDG sowohl Sicherheits- als auch Legitimationsvorfälle beinhaltet. **Sicherheitsvorfälle** sind Vorfälle, Feststellungen, Ereignisse, Versäumnisse oder dergleichen, die die Informationssicherheit betreffen und dabei vor allem die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten gefährden. **Legitimationsvorfälle** sind Vorfälle, Feststellungen, Ereignisse, Versäumnisse oder dergleichen, die zeigen, dass städtische Behörden oder Verwaltungseinheiten Personendaten bearbeiten, ohne hierfür über die erforderliche Legitimation (Rechtsgrundlage, Einwilligung) zu verfügen.

Klärung weiterer rechtlicher Fragen

Adressat der Meldepflicht nach IDG sind «die verantwortlichen öffentlichen Organe». Darunter sind in erster Linie die Verwaltungseinheiten des Kantons und der Gemeinden zu verstehen. Für die Stadt Zürich sind dies in erster Linie die Departemente, Dienstabteilungen sowie Fachstellen.

Meldepflichtige Vorfälle werden in der Praxis nicht von (abstrakten) Organisationseinheiten festgestellt, sondern von (natürlichen) Personen, insbesondere von Angestellten. Es stellt sich somit die Frage, welche Rechte und Pflichten den Angestellten in Zusammenhang mit der Meldepflicht zukommen. An wen müssen relevante Feststellungen gemeldet werden? Direkt an die Datenschutzstelle oder an interne Stellen? Welche Rechte oder Pflichten haben Angestellte, wenn intern mit Meldungen nicht korrekt umgegangen wird? In welchem **Verhältnis** steht die **Meldepflicht** nach IDG zum Amtsgeheimnis und **zu personalrechtlichen (Verschwiegenheits- oder Loyalitäts-)Pflichten?** Diese und weitere Fragen sind erkannt und werden vom Stadtrat und den verantwortlichen Verwaltungseinheiten entsprechend geklärt.

Merkblatt der Datenschutzstelle

Die Datenschutzstelle hat zur Meldepflicht nach IDG ein Merkblatt verfasst und im städtischen Fachintranet Datenschutz publiziert. Das Merkblatt beschreibt und konkretisiert soweit wie möglich, welche Vorfälle meldepflichtig sind, was eine Meldung beinhalten muss, wann und wie die Meldung zu erfolgen hat und in welchen Fällen betroffene Personen zu informieren sind.

Fragebogen Quellensteuer

Der nachfolgend beschriebene Vorfall ereignete sich, kurz bevor die neue Meldepflicht ins IDG eingeführt wurde. Er zeigt auf, dass die Meldepflicht, so wie sie seit Juni 2020 besteht, mit guten Gründen nicht auf Vorfälle der Informationssicherheit zu beschränken ist. Auch gravierende Vorfälle, bei denen sich zeigt, dass Verwaltungsstellen **ohne genügende Legitimation** sensible Personendaten erheben und bearbeiten, sind zu melden, damit von unabhängiger Stelle erforderliche Massnahmen zum Schutz der Grund- und Persönlichkeitsrechte Betroffener verlangt und überprüft werden können.

Die Stadtverwaltung Zürich ist gemäss Steuergesetz verpflichtet, Daten ihrer Angestellten, welche unter die Quellensteuerpflicht fallen, für das kantonale Steueramt zu erheben und an dieses weiterzuleiten. Die Erhebung dieser Daten erfolgt mittels eines Fragebogens, der von einer städtischen Verwaltungsstelle eigens hierfür erstellt wurde.

Im Berichtsjahr musste aufgrund einer **Reklamation eines betroffenen städtischen Mitarbeiters** bei der Datenschutzstelle festgestellt werden, dass mit dem Fragebogen Daten erfragt werden, die für den Vollzug der Quellensteuer nicht erforderlich waren. Die Datenschutzstelle machte sich gemeinsam mit der verantwortlichen Dienstabteilung an die Aufarbeitung und Korrektur des Fragebogens.

In einem ersten Schritt wurde analysiert und rechtlich abgeklärt, welche Daten im Kontext der Quellensteuerpflicht von der städtischen Verwaltung erhoben werden müssen und welche eben gerade nicht hätten erfragt werden dürfen. Es stellte sich heraus, dass es sich bei den fälschlicherweise erhobenen Informationen um **sensible Daten** handelt, welche die Familienkonstellation und die Intimsphäre der Betroffenen tangierten. In der Folge wurden alle Fragen bzw. Themen aus dem Fragebogen entfernt, welche das Steueramt nicht für die Veranlagung von quellensteuerpflichtigen Mitarbeitenden benötigt.

Als nächsten Schritt wurde evaluiert, was mit den bereits eingesetzten physischen und digitalisierten Fragebögen passieren soll. Diese enthielten ja einerseits korrekte Daten, welche im Zusammenhang mit der Quellensteuer erhoben und aufbewahrt werden müssen, andererseits aber auch Daten, welche nicht hätten erhoben werden dürfen. Aufgrund der Aufbewahrungspflicht für diese Fragebögen kam eine gänzliche Vernichtung derselben nicht in Frage. Damit dennoch das Risiko für (weitere) Persönlichkeitsverletzungen so klein wie möglich gehalten wird, verlangte die Datenschutzstelle zwei auf den vorliegenden Fall zugeschnittene Massnahmen: Eine **strenge Zugriffsbeschränkung** sowie eine **Schwärzung der widerrechtlich erhobenen Daten,** wann immer auf einen Fragebogen zugegriffen wird. Die verantwortliche Dienstabteilung hat beide Massnahmen implementiert.

Feststellungen

Datenschutz in Zeiten von Covid

Damit die Covid-Pandemie erfolgreich bewältigt werden kann, spielen auch Informationen und Daten eine zentrale Rolle. Für **Contact-Tracing, Testen** oder **Impfen** werden zum Teil sensible Personendaten erhoben und weiterbearbeitet. Diese Daten tangieren nicht nur die direkt betroffenen Personen, die beispielsweise das Covid-App auf ihrem Handy installiert haben oder sich testen oder impfen lassen. Sie bilden auch die Grundlage für zahlreiche Erhebungen und Auswertungen, um geeignete Massnahmen zur Bekämpfung der Covid-Pandemie festzulegen. Für die Erhebung und Bearbeitung der hierfür benötigten – personenbezogenen oder anonymisierten – Daten sind **in erster Linie der Bund, die Kantone oder Private** zuständig. Aus diesem Grund gab es in der Stadtverwaltung nur wenige Vorhaben oder Projekte, die eine Bearbeitung von Personendaten aufgrund von Contact-Tracing, Testen oder Impfen mit sich brachten. Einbezogen wurde die Datenschutzstelle in zwei Terminbuchungsplattformen für Covid-Testangebote sowie in die Erfassung von Kontaktdaten von Besucherinnen und Besuchern städtischer Pflegeinstitutionen. Diese Vorhaben wurden über den üblichen städtischen ISDS-Prozess (vgl. Grundlagen **Seite 9**) geprüft.

Stärker wirkte sich die Covid-Pandemie in anderer – indirekter – Hinsicht auf den Umgang der Stadtverwaltung mit Informationen und Personendaten aus. Wenn quasi von heute auf morgen nicht mehr im Büro gearbeitet und nicht mehr in der Schule unterrichtet werden kann, braucht es rasch technische Lösungen, um dennoch arbeiten, unterrichten und kommunizieren zu können. Unter solchen ausserordentlichen Umständen muss allenfalls von gewissen Anforderungen, die üblicherweise an den Umgang mit Informationen gestellt werden, abgewichen werden können. Welche Abweichungen dabei zu rechtfertigen sind, muss im Einzelfall evaluiert und anhand von Risikoanalysen abgeschätzt werden. Ein wertvolles Hilfsmittel für die hierfür erforderlichen Prüfungen stellt die Datenschutzbeauftragte des Kantons Zürich in Zusammenarbeit mit weiteren Datenschutzstellen zur Verfügung. Auf deren **Webseite** ist eine **Liste** mit Apps, Plattformen oder Systemen publiziert, die vorübergehend und allenfalls unter Auflagen eingesetzt werden können, auch wenn sie die datenschutzrechtlichen Anforderungen nur zum Teil erfüllen. Die Liste weist ausdrücklich darauf hin, dass stets eine **konkrete Risikoanalyse** durchzuführen ist und die **Verantwortung** auch in Zeiten von Covid stets bei derjenigen Verwaltungsstelle liegt, die den Dienst oder das Produkt einsetzt.

Für die Zeit nach der Covid-Ausnahmesituation muss eine Rückkehr zum «Normalbetrieb» stattfinden, so dass Abweichungen von gesetzlichen Anforderungen auf alle Fälle nur einen **temporären und provisorischen Charakter** haben. Dies verlangt auch, dass für dringlich eingeführte Apps, Plattformen oder Systeme, ohne die ein Verwaltungs- oder Schulbetrieb nicht hätte gewährleistet werden können, die üblichen städtischen Prüfungen nachgeholt werden.

Dass auch trotz Dringlichkeit datenschutzkonforme Lösungen realisiert werden können, zeigte ein Beispiel aus dem Berichtsjahr. Eltern eines Kindes in der Volksschule beschwerten sich bei der Datenschutzstelle über eine **Lernplattform,** die die Schule ihres Kindes für den Unterricht im Home-Schooling einsetzte und auf welcher sich die Schülerinnen und Schüler registrieren mussten. Grund der Beschwerde war nicht die Lernplattform als solche, sondern vielmehr die **Analyse- und Tracking-Tools,** die in diese Plattform eingebunden waren. Die eingesetzten Tools gehören zu denjenigen, die regelmässig kritisiert werden, weil sie die Privatsphäre der Nutzerinnen und Nutzer durch intransparente Datensammlungen und Profilanlegungen zu wenig respektieren und dem europäischen und schweizerischen Persönlichkeits- und Datenschutzrecht nicht genügen. Dieses Defizit widerspiegelte sich auch in der **Datenschutzerklärung** der Lernplattform. Diese war wenig informativ und nur schwer verständlich formuliert, so dass nicht erkennbar war, welche Daten über die Schülerinnen und Schüler in welcher Weise bearbeitet werden. Dank einer gewissen Hartnäckigkeit seitens Datenschutzstelle und KITS-Fachstelle des Schulamtes konnte erreicht werden, dass der Anbieter der Lernplattform die kritisierten Analyse- und Tracking-Tools entfernte und durch datenschutzfreundliche ersetzte.

Interview

«Mein Konto» und E-Government der Stadt Zürich

Die Datenschutzstelle hat in ihren letzten Tätigkeitsberichten regelmässig «Mein Konto», das zentrale Zugangsportal für die städtischen Online-Dienste, thematisiert. Mit diesem Portal vereinfacht die Stadt Zürich sukzessive den Zugang der Bevölkerung zu den Dienstleistungen der Verwaltung. Findet «Mein Konto» Anklang bei der Bevölkerung? Erreicht man die Stadtverwaltung bald nur noch in digitaler Form? Und wie steht es dabei um den Datenschutz und die Datensicherheit? Diese und weitere Fragen beantwortet

Michael Keller, Abteilungsleiter E-Government & Digitale Prozesse bei der städtischen Dienstabteilung Organisation und Information Stadt Zürich (OIZ).

Welche Bedeutung hat «Mein Konto» für das E-Government bzw. die Digitalisierung der Stadt Zürich?

Das «Mein Konto» darf sicherlich als wichtiges Element im grossen Thema Digitalisierung bezeichnet werden. Es ist Dreh- und Angelpunkt, um Verwaltungsgeschäfte online abwickeln zu können. Vor kurzem wurde die 100 000er Marke von registrierten Nutzenden erreicht. Pro Monat kommen rund 4000 neue Nutzende hinzu. Auch die Mitteilungsfunktion in «Mein Konto» wird rege genutzt: ca. 70 000 Mitteilungen werden pro Monat über die Plattform verschickt. Der vor ein paar Monaten lancierte Online-Service «Steuern verwalten» zählt bereits über 10 000 Registrierungen. Diese Zahlen zeigen, dass die Nachfrage und das Bedürfnis nach städtischen Online-Angeboten bestehen.

Was weiss die Stadt Zürich darüber, wie «Mein Konto» bei der Bevölkerung ankommt? Gibt es dazu Feedback, Anliegen, Wünsche?

Wir erhalten viel positives Feedback zu unseren Online-Dienstleistungen. Natürlich gibt es auch kritische Rückfragen:

«Sind meine Daten sicher? Weshalb kann das «Mein Konto» kein Englisch?» Durch stetes Weiterentwickeln von «Mein Konto» berücksichtigen wir Kundenwünsche, wir fokussieren uns dabei auf solche Optimierungen, die für die Bevölkerung den grössten Nutzen bringen.

Was sollte «Mein Konto» in Zukunft können, was es heute noch nicht kann? Wohin geht die Reise?

Heute sind 37 Services online und es kommen immer mehr aus allen Bereichen der Stadtverwaltung dazu. Das ist erfreulich. Insbesondere bei den Online-Services für Eltern und Erziehungsberechtigte sind wir schon sehr gut unterwegs. Im Bereich Juristische Personen haben wir sicherlich das grösste Potential. Wichtig ist, dass wir stetig dranbleiben und Inputs aus der Bevölkerung aufnehmen und auch umsetzen.

Laut dem E-Government-Monitor 2020 nutzen Herr und Frau Schweizer durchschnittlich dreimal im Jahr einen elektronischen Behördendienst. Dabei wählen sie vor allem den Online-Weg, wenn sie Informationen zu Zuständigkeiten oder Öffnungszeiten der Behörden erhalten möchten, um Formulare herunterzuladen oder die Steuererklärung auszufüllen. Klingt nicht gerade nach digitalisierter Gesellschaft und Verwaltung. Wie beurteilen Sie dies?

Das muss differenziert betrachten werden. Wenn ich Kinder in der Schule habe oder ein Bauprojekt plane, habe ich viel mit der Verwaltung zu tun. Lebe ich als Studentin in einer WG, habe ich ausser den Steuern kaum Kontakt mit der Verwaltung. Auch wenn viele Studien sagen, dass die Schweiz nicht vorne dabei ist, möchte ich aus Sicht Stadt Zürich dem widersprechen. Wir bieten mittlerweile viele Services digital an, seit letztem Herbst auch bei den Themen Bauen und Steuern, um bei den Beispielen zu blieben. Nicht zu vergessen ist übrigens das breite Angebot der Stadt Zürich beim Open Government Data. Da können wir international absolut mithalten. Die Corona-Pandemie hat zudem die Nutzung und die Nachfrage von städtischen Online-Angeboten verändert. Online-Services, wie z. B. Online-Umzugsmeldungen, wurden in der Zeit verstärkt genutzt.

Wird nach den Gründen gefragt, die gegen eine Nutzung von Online-Diensten sprechen, nennen die Befragten regelmässig den Datenschutz an erster Stelle. Was muss sich ändern, damit die Bevölkerung mehr darauf vertrauen wird, dass die Stadtverwaltung datenschutzkonform handelt?

Wir glauben, dass bereits heute ein grosser Teil der Nutzenden der Verwaltung vertraut. Wir bekommen in unseren Gesprächen mit der Bevölkerung immer wieder diese Rückmeldung: «Wir vertrauen der Stadt Zürich». Diesem Vertrauen müssen wir sehr Sorge tragen. Datensicherheit und Datenschutz ist bei allen IT-Vorhaben der Stadt Zürich zentral und jedes einzelne Projekt muss einen entsprechenden Prozess durchlaufen. Werden die definierten Kriterien zu Datenschutz und Datensicherheit nicht erfüllt, kann der Service nicht live gehen. Zusätzlich finden in der OIZ regelmässige externe Sicherheitsaudits statt. Und unser eigenes Security Operation Center überwacht die Services rund um die Uhr auf potentielle Angriffe. Betreffend Datenschutz gilt für die Nutzenden unserer Online-Services folgendes Prinzip: «Mein Konto – meine Daten». Bundesrätin Sommaruga sagte 2014:«Ein gutes digitales Angebot der Verwaltung schafft Vertrauen in die Behörde/Staat». Dem schliessen wir uns an.

Was bedeutet die Ablehnung der E-ID durch die Stimmbürgerinnen und Stimmbürger für die Weiterentwicklung des E-Government bzw. der Digitalisierung Stadt Zürich?

Dies ist sicherlich bedauerlich, dass keine einheitliche, schweizweite Lösung gefunden wurde. Ich bin aber überzeugt, dass mittelfristig die Schweiz über eine elektronische Identität verfügen wird. Bis dahin schauen wir, dass wir unseren Nutzenden einfache Lösungen anbieten können. Wie beispielsweise die «Zürich Access»-App, die wir diesen Februar lanciert hatten. Nicht vergessen darf man, dass es auf gesetzlicher Ebene noch viel zu tun gibt. Doch da ist der Kanton mit der neuen Gesetzgebung «DigiLex» zur Schaffung rechtlicher Grundlagen für den elektronischen Geschäftsverkehr aktiv.

Es gibt Menschen, die mit der Digitalisierung nicht mithalten können oder wollen. Eine Kommunikation mit der Verwaltung nur über das Internet oder mit Mobilgeräten ist für sie nicht möglich. Wie geht die Stadt Zürich damit um?

Eine Gegenfrage: was wäre, wenn wir gewisse Bevölkerungsschichten ausschliessen würden beispielsweise wegen einer Mobilitätseinschränkung oder weil sie in der Nacht arbeiten? Wir müssen als Stadt Zürich alle Bevölkerungsgruppen berücksichtigen. So erhalten beispielsweise Personen, die mit der digitalen Welt noch nicht so vertraut sind, beim Verwenden von digitalen Services Unterstützung im Stadthaus. Ein anderes Beispiel: Zurzeit prüfen wir, wie die fremdsprachige Bevölkerung unsere Online-Services in ihrer Muttersprache nutzen kann. Technische Lösungen gibt es, wie weit diese unserem hohen Qualitätsstandard genügen, evaluieren wir gerade.

Im Berichtsjahr setzte sich die Datenschutzstelle personell wie folgt zusammen:

Marcel Studer, RA lic. iur.
Wirtschaftsinformatiker NDS
Datenschutzbeauftragter (100 %)

Patrizia Zbinden, Dr. iur.
juristische Mitarbeiterin (60 %)

Katrin Gisler, MLaw
juristische Mitarbeiterin (80 %)

Jürg von Flüe, lic. iur.
juristischer Mitarbeiter (60 %)

Lindita Dzaferi
Sekretariat (20 %)

Impressum

Herausgeberin
Stadt Zürich
Datenschutzstelle
Beckenhofstrasse 59
8006 Zürich

Mai 2021

Auflage
80 Exemplare, gedruckt auf 100 % Recyclingpapier

Druck
PrintShop, Stadt Zürich

Gestaltung
Züriblau, Stadt Zürich

Stadt Zürich
Datenschutzstelle
Beckenhofstrasse 59
8006 Zürich
T +41 44 412 16 00
datenschutz@zuerich.ch
stadt-zuerich.ch/datenschutz