Stadt Zürich
Datenschutzstelle

2019

Geschätzte Leserinnen und Leser

Rund die Hälfte der Stadtzürcherinnen und Stadtzürcher ist der fortschreitenden Digitalisierung unserer Gesellschaft positiv gegenüber eingestellt. Dies zeigte die Bevölkerungsbefragung der Stadt Zürich 2019. Die andere Hälfte der Stadtbevölkerung sieht im technologischen Wandel keinen positiven oder sogar einen negativen Einfluss auf ihr Privatleben. Einen vergleichsweise höheren Stellenwert hat die Digitalisierung in der Stadtverwaltung. Mittlerweile reicht die Stadtverwaltung der Datenschutzstelle kaum noch ein Vorhaben oder ein Projekt im Bereich Information und Kommunikation zur Prüfung ein, welches nicht im Kontext von «Digitalisierung» oder «Digitale Stadt» steht. Es erstaunt deshalb nicht, dass die Digitalisierung auch im vorliegenden Tätigkeitsbericht eine Hauptrolle spielt.

Eindeutiger als das Verhältnis der Stadtzürcherinnen und Stadtzürcher zur Digitalisierung ist ihre Haltung zum Datenschutz. Mit grosser Mehrheit haben sie sich dahingehend geäussert, dass ihnen der Schutz ihrer sensiblen Daten sehr wichtig oder mindestens wichtig ist. Auch dies bringt die Bevölkerungsbefragung der Stadt Zürich 2019 zum Ausdruck. Diese klare Aussage der Stadtbevölkerung freut uns sehr und motiviert uns – aber sicher auch die gesamte Stadtverwaltung – in unserer täglichen Arbeit. Herzlichen Dank dafür.

Wir wünschen Ihnen eine informative Lektüre und danken Ihnen für Ihr Interesse.

Datenschutzstelle Stadt Zürich
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
  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 über 60 Projekte oder Vorhaben zur Prüfung und Beratung zu. Eine so grosse Anzahl an Neuanmeldungen via ISDS-Prozess gab es bisher noch nie.

– 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 regelmässig von Mitarbeitenden aus der Stadtverwaltung um Beratung oder Abklärung zu datenschutzrechtlichen Belangen in Zusammenhang mit dem Arbeitsplatz angefragt. Dabei geht es oft um die Frage, unter welchen Voraussetzungen und in welchem Ausmasse Vorgesetzte das Verhalten ihrer Angestellten überwachen dürfen. Weitere Ausführungen zum Thema Personalbereich folgen im entsprechenden FOKUS-Beitrag ab Seite 32.

– 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. Allgemeine Fragen zum Datenschutzrecht beantwortet die Datenschutzstelle regelmässig am Telefon oder per E-Mail.

– Videoüberwachung der Stadtverwaltung überprüfen
  Das Thema Videoüberwachung hat sich für die Datenschutzstelle zu einem eigentlichen Schwerpunktthema entwickelt. 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. Darüber hinaus stellen

auch Privatpersonen bei der Datenschutzstelle Anfragen zu Videoüberwachung. Weitere Ausführungen zum Thema Videoüberwachung folgen im entsprechenden FOKUS-Beitrag ab Seite 52.

– 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 Verantwortlichen 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. Weitere Ausführungen zum Thema Datenschutzrecht folgen im entsprechenden FOKUS-Beitrag ab Seite 59.

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 ein Gesetz, d. h. 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 Personen 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

FOKUS DIGITALISIERUNG DER STADTVERWALTUNG

Die Digitalisierung der Stadtverwaltung ist seit Jahren fester Bestandteil städtischer Strategien: Bereits vor fünf Jahren bezeichnete der Stadtrat in der Strategie Zürich 2035 die «Digitale Stadt» als eines der Handlungsfelder für die Herausforderungen der Zukunft. In der IT-Strategie der Stadt Zürich 2016 wurde die Digitalisierung als eine der strategischen Stossrichtungen identifiziert und im Berichtsjahr beschloss der Stadtrat, die digitale Transformation in der Stadtverwaltung mit der Umsetzung und Konkretisierung des Strategie-Schwerpunktes «Digitale Stadt» zu verstärken und zu beschleunigen. Mit Hilfe der Digitalisierung verspricht er sich, den Austausch mit der Bevölkerung, den Unternehmen und weiteren Anspruchsgruppen zu vereinfachen und schneller und komfortabler zu gestalten. Darüber hinaus soll die Digitalisierung verwaltungsintern die effizientere Gestaltung von Prozessen ermöglichen.

Gegliedert in thematische Teilbereiche beschreibt der Stadtrat zahlreiche städtische Vorhaben und Projekte, auf welche sich der Strategie-Schwerpunkt «Digitale Stadt» fokussiert. Bei diesen Vorhaben und Projekten – beispielsweise «Mein Konto», Cockpit für Steuerpflichtige, Digitalisierung und Schulen, Digitaler Posteingang, E-Rechnung, Cloud, Datenanalyse und zahlreiche mehr – gibt es kaum eines, in welches die Datenschutzstelle nicht bereits in der einen oder anderen Art involviert war bzw. ist. In der Regel geschieht der Einbezug der Datenschutzstelle via städtischem ISDS-Prozess (vgl. Einleitungstext Seite 8) oder durch unmittelbare Mitwirkung der Datenschutzstelle in den entsprechenden Projekten, so vor allem bei Vorhaben mit eher regulatorischem Charakter.

Im letzten Teilbereich des Strategie-Schwerpunkts «Digitale Stadt» hält der Stadtrat fest, dass in der Stadt Zürich Digitalisierungskompetenzen auf- und ausgebaut werden müssen. Das entsprechende Know-how fehle zum Teil noch und sei Bedingung, damit die Potenziale der Digitalisierung erkannt und genutzt werden können. Zu diesen Kompetenzen müssen unserer Ansicht nach auch die Sensibilisierung und das Wissen in Bezug auf die datenschutzrechtlichen Fragen und Anforderungen gehören, die sich spezifisch bei Digitalisierungsvorhaben ergeben. Die nachfolgend erwähnten Beispiele aus dem Berichtsjahr zeigen, dass die Stadtverwaltung mit Digitalisierungsvorhaben wie beispielsweise der Konzipierung von Mobile Apps oder dem Einsatz von Künstlicher Intelligenz erst am Beginn der digitalen Transformation steht und es wichtig ist, dass sie in den Aufbau entsprechender Kompetenzen investiert. Auch der Datenschutzstelle ist dies ein Anliegen und sie sorgt deshalb beispielsweise durch vermehrten Einbezug der Rechtsdienste in die jeweiligen Projekte dafür, dass das datenschutzrechtliche Know-how nicht nur bei ihr, sondern auch in den Dienstabteilungen und Departementen auf- und ausgebaut wird.

Künstliche Intelligenz in der Verwaltung

Künstliche Intelligenz (KI) ist bereits seit einigen Jahren ein Trend (-thema) in verschiedenen Branchen und Wirtschaftszweigen. Auch in der (städtischen) Verwaltung ist KI mittlerweile angekommen und kommt – wenn auch vorerst eher zögerlich – in ersten Bereichen zum Zug. KI kann im verwaltungsspezifischen Kontext vieles leisten: Beispielsweise Mitarbeitende bei der Erfüllung ihrer Aufgaben unterstützen oder zur Qualitätssicherung beitragen. Die Anwendung von KI kann für die Verwaltung in diversen Bereichen einen Effizienzgewinn bringen. Dabei gilt es jedoch immer die datenschutzrechtlichen Vorgaben zu beachten und diese sowohl in den Prozessen von KI als auch in deren Ergebnissen umzusetzen.

Was ist KI eigentlich?

Laut Wikipedia ist unter Künstlicher Intelligenz ein Teilgebiet der Informatik zu verstehen, welches sich mit der Automatisierung intelligenten Verhaltens und dem maschinellen Lernen befasst. So versucht KI insbesondere, kognitive Fähigkeiten wie Lernen, Planen oder Problemlösen in Computersystemen zu verwirklichen. Eine allgemein gültige Definition von KI existiert jedoch nicht. Anstelle einer Definition kann Künstliche Intelligenz folgendermassen charakterisiert werden: KI-Systeme sind in der Lage, eine grosse Menge an komplexen Daten in einer Form auszuwerten, die mit anderen Technologien nach heutigem Stand nicht möglich wäre. KI-Systeme können mit Hilfe von (teilweise selbständig lernenden) Algorithmen Muster in Daten erkennen und Vorhersagen machen. Sie sind in der Lage, komplexe Probleme zu lösen, die bisher dem Menschen vorbehalten waren und agieren dabei weitgehend autonom.

Was hat KI mit Daten(schutz) zu tun?

Was bei jeder Datenbearbeitung gilt, ist auch beim Einsatz von Künstlicher Intelligenz zu beachten: Immer dann, wenn nicht nur bloss Sach-, sondern auch Personendaten bearbeitet werden, müssen die Grundsätze des Datenschutzes eingehalten werden. Der Einsatz von KI bringt jedoch im Vergleich zu anderen Technologien eine weitere datenschutzrechtlich relevante Dimension mit sich. Die zunehmende Fähigkeit, verschiedene Datensätze zu verknüpfen, kann dazu führen, dass aus bestehenden Daten neue Daten entstehen, welche ohne den Einsatz von KI nicht entstanden wären. Diese Entwicklung stellt die Verwaltung vor neue Herausforderungen, da auch diese neuen Daten bzw. nur schon die (gewollte oder ungewollte) Möglichkeit, neue Daten zu schaffen, in Einklang mit den datenschutzrechtlichen Prinzipien gebracht werden müssen. Dabei geht es insbesondere um die Prinzipien der Gesetzmässigkeit (Ist die Verwaltung berechtigt, mit KI neue Personendaten zu generieren?), der Zweckbindung (Wie wird sichergestellt, dass mit KI Personendaten nicht zu anderen als den gesetzlich vorgesehenen Zwecken bearbeitet werden?), der Verhältnismässigkeit (Beschränkt sich die Verwaltung auch mit KI auf die erforderlichen Personendaten?) und der Transparenz (Ist bekannt und nachvollziehbar, welche zusätzlichen Personendaten mit KI generiert und bearbeitet werden?).

KI wirft zudem Fragen und Probleme auf, die weit über den Datenschutz hinausgehen. Dazu gehört die Problematik der potentiellen Diskriminierung durch den Einsatz von Künstlicher Intelligenz. Diese Gefahr besteht insbesondere immer dann, wenn die dem Algorithmus zugrundeliegenden Daten von geringer Qualität sind und/oder diesen Daten eine bereits vorhandene Diskriminierung innewohnt, diese mit anderen Worten nicht «neutral» sind.

KI benötigt Transparenz und Nachvollziehbarkeit

Eine (nicht nur) datenschutzrechtliche Anforderung ist, dass KI transparent, nachvollziehbar und erklärbar sein muss. Insbesondere aus rechtsstaatlicher Sicht sind Vorkehrungen zu treffen, wie die Transparenz bei KI-basierten Entscheidungen gefördert werden kann.

Wird ein KI-Algorithmus so eingesetzt, dass dieser unmittelbar selbst eine verbindliche Entscheidung trifft, dann besteht die Gefahr, dass der Anspruch auf rechtliches Gehör beeinträchtigt wird. Der Entwurf zur Revision des Datenschutzgesetzes des Bundes (DSG) trägt dieser Problematik bei vollautomatisierten Entscheidungen Rechnung. Trifft ein Bundesorgan eine Entscheidung, die ausschliesslich aufgrund einer automatisierten Bearbeitung personenbezogener Daten getroffen wird und die rechtliche Auswirkungen auf eine betroffene Person hat, muss diese transparent informiert werden. Die betroffene Person kann zudem verlangen, dass die Entscheidung von einer natürlichen Person überprüft oder dass ihr die Logik mitgeteilt wird, auf der die Entscheidung beruht. Ähnliches sieht bereits die Datenschutzgrundverordnung der EU vor, wohingegen das Datenschutzrecht des Kantons Zürich keine derartige Regelung kennt. Ein mögliches Beispiel für eine solch vollautomatisierte Entscheidung wäre im Kontext der Verwaltung etwa die Verhängung einer Busse für eine Geschwindigkeitsübertretung ausschliesslich auf Grundlage von Fotografien des Kennzeichens und der Person am Steuer sowie automatischer Hinzuziehung von Daten aus dem Fahrzeugregister.

Gemäss des DSG-Revisionsentwurfs des Bundes besteht keine Mitteilungspflicht der Behörden, wenn Verwaltungsangestellte in die Entscheidungsfindung eingreifen und wenn die Künstliche Intelligenz lediglich als Entscheidungshilfe dient. Dennoch bestehen spezielle Anforderungen an die Nachvollziehbarkeit auch bei nicht vollautomatisierten Entscheidungen von Verwaltungen, welche mithilfe von KI getroffen werden und die Rechtsstellung einer Person betreffen. Aus dem verfassungsrechtlichen Anspruch auf rechtliches Gehör leitet sich die Pflicht der Behörden ab, ihre Entscheide zu begründen. Stützt sich eine Behörde für ihren Entscheid auf KI ab, muss sie Auskunft über die im KI-System berücksichtigten Informationen, die getroffenen Annahmen und die massgebenden Kriterien für das Ergebnis geben können. Eine solche KI-gestützte, aber nicht vollautomatisierte Entscheidung liegt beispielsweise dann vor, wenn Verwaltungsangestellte durch den Einsatz eines KI-Systems bestimmte Entscheidhilfen oder Visualisierungen von Prozessen erhalten, welche sie bei ihrer Arbeit unterstützen.

KI benötigt technische und organisatorische Standards

Datenschutz und Datensicherheit gehen bekanntlich Hand in Hand. Bei KI-Systemen trifft dies in besonderem Masse zu, da sie im digitalen Umfeld ausgeführt werden. So müssen beim Einsatz von KI technische und organisatorische Massnahmen getroffen werden, welche eine effiziente Datensicherheit gewährleisten. Für einen datenschutzkonformen Einsatz von KI-Systemen gibt es aktuell noch keine speziellen Standards oder detaillierten Anforderungen. Jedoch ist bei der Entwicklung von KI-Systemen stets darauf zu achten, den Grundsätzen des Privacy by Design und Privacy by Default zu folgen (diese Grundsätze werden auf den Seiten 25 und 27 genauer erläutert).

Einsatz von KI in der Stadtverwaltung Zürich

Im Bereich des Personal Recruitings hatte die Datenschutzstelle im Berichtsjahr ein Projekt zu beurteilen, welches den Einsatz eines sogenannten Chatbots zum Gegenstand hatte. Ein Chatbot oder kurz Bot ist ein textbasiertes Dialogsystem, welches das Chatten mit einem technischen System erlaubt. Die Dienstabteilung plante, offene Fragen von Stellenbewerbenden mittels Chatbot beantworten zu lassen. Da es möglich ist, mit einem Chatbot wie mit einem Menschen zu sprechen, ist es für Betroffene unter Umständen nicht erkennbar, dass es sich um eine Maschine handelt. Die Datenschutzstelle legte bei der Beurteilung des Projekts grossen Wert auf eine vorherige und transparente Information der betroffenen Personen über eine solche Interaktion mit Systemen der Künstlichen Intelligenz.

Ebenfalls im Berichtsjahr befasste sich die Datenschutzstelle mit einem Projekt des Steueramtes, welches die automatisierte Verarbeitung von Steuerdaten zum Zweck von Veranlagungsentscheidungen vorsieht. Bei diesem Vorhaben soll mittels KI-Analyse der Daten eine Entscheidungsempfehlung für den Steuersachbearbeiter vorbereitet werden. Es handelt sich somit nicht um eine vollautomatisierte Entscheidung, dennoch besteht das Bedürfnis, KI-basierte Entscheidungen (in vorliegendem Fall die Entscheidungsempfehlung) hinterfragen zu können. Für die Datenschutzstelle war es deshalb auch in diesem Projekt von Wichtigkeit, dass die Betroffenen transparent und nachvollziehbar informiert werden.

Allgemein kann gesagt werden, dass – nebst den übrigen datenschutzrechtlichen Anforderungen wie Gesetzmässigkeit, Zweckbindung, Verhältnismässigkeit und Datensicherheit – eine transparenzschaffende Kennzeichnung von KI-gestützten Verwaltungsentscheidungen zentral ist. Denn nur dadurch erhält die von einer Entscheidung betroffene Person die Möglichkeit, die Korrektheit der Entscheidung zu hinterfragen. Wie diese Forderung nach einer transparenzschaffenden Kennzeichnung von der Verwaltung konkret umgesetzt werden muss, ist derzeit jedoch noch nicht geklärt und es wird sich erst mit der Entwicklung des Rechts im KI-Bereich und der sich daraus ergebenden Rechtsprechung zeigen, wie eine solche Kennzeichnung ausgestaltet sein muss.

In der städtischen Verwaltung steht der Einsatz von KI erst am Anfang und betrifft bisher eher unproblematische Daten und Bereiche. Für die Verwaltung, aber auch die Datenschutzstelle, gilt es nun Erfahrungen zu sammeln und sich den neuen Herausforderungen, welche aus datenschutzrechtlicher Optik im Zusammenhang mit dieser neuen Technologie auf sie zukommen, zu stellen. Bisher macht es den Eindruck, dass sowohl mit den rechtlichen Vorgaben im Datenscwhutz, als auch mit dem städtischen ISDS-Prozess (vgl. Einleitungstext Seite 8), welcher zu einer frühen Prüfung eines jeden IT-Projekts führt, diesen neuen Herausforderungen adäquat begegnet werden kann.

Mobile Apps der Stadtverwaltung

Das Leben ohne Smartphone und die damit verbundene Nutzung praktischer Apps ist für viele Menschen heute kaum mehr vorstellbar. Auch die Stadtverwaltung Zürich bietet diverse Dienstleistungen mittels Mobile App an. So gibt es unter anderem die Entsorgungs-App, die WC-Finder-App oder die Air-Check-App, die Interessierte über die aktuelle Luftqualität der Stadt Zürich informiert. Neben diesen vergleichsweise harmlosen Apps hat die Stadtverwaltung im Berichtsjahr auch eine App konzipiert, welche sensible Personendaten speichert und bearbeitet. Die Datenschutzstelle kontrollierte die Neuentwicklung dieser App, welche Drogensüchtige in ihrer Therapie unterstützt.

Konzipierung und Planung

Es ist wichtig, das Thema Datenschutz bereits zu Beginn der Konzeption einer App auf dem Radar zu haben und nicht erst bei der bereits fertig erstellten App zu kontrollieren, ob diese datenschutzkonform ist. Denn nur wenn zu Beginn der App-Entwicklung die wichtigen Fragen geklärt und die richtigen Weichen gestellt sind, kann sichergestellt werden, dass städtische Apps den datenschutzrechtlichen Vorgaben entsprechen. Bereits in der Planung der App ist auf eine konsequente Umsetzung des Grundsatzes Privacy by Design zu achten. Übersetzt heisst Privacy by Design «Datenschutz durch Technikgestaltung» und greift den Gedanken auf, dass sich Datenschutz nur einhalten lässt, wenn er bereits bei Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert ist. Mit anderen Worten: Der Schutz personenbezogener Daten erfolgt durch das frühzeitige Ergreifen technischer und organisatorischer Massnahmen im Entwicklungsstadium.

Dreh- und Angelpunkt bei der Prüfung von Apps ist wie bei jeder Datenbearbeitung die Bewertung der Personendaten, die bearbeitet werden. Die Sensitivität der Daten bestimmt, unter welchen rechtlichen Voraussetzungen die Verwaltung eine App einsetzen darf und welche technischen Schutzmassnahmen sie hierfür ergreifen muss. Werden sensible Personendaten in der App bearbeitet, ist beispielsweise eine Zwei-Faktor-Authentifizierung für das Starten und Entsperren der App notwendig oder es ist zu verlangen, dass die Daten verschlüsselt übertragen und gespeichert werden. Je nachdem kann den Nutzern und Nutzerinnen auch die Möglichkeit gegeben werden, die Schutzmassnahmen individuell anzupassen. Wie bei jeder Bearbeitung von Personendaten darf auch bei der Konzipierung einer App nicht übersehen werden, dass nur diejenigen Personendaten bearbeitet werden, die zu dem jeweilig mit der App verfolgten Zweck erforderlich sind.

Transparenz und Grundeinstellung

Bevor die App installiert wird, müssen die Nutzer und Nutzerinnen mittels Datenschutzerklärung transparent über die Datenbearbeitung informiert werden. Erst wenn sie dieser aktiv zustimmen, darf die Verwaltung Daten mittels App bearbeiten. Eine Datenschutzerklärung muss so verfasst und platziert sein, dass die Nutzer und Nutzerinnen diese lesen und auch verstehen. Damit eine Datenschutzerklärung als transparent angesehen werden kann, muss sie diverse Angaben enthalten. So muss daraus erkennbar sein, welches öffentliche Organ welche Personendaten zu welchem Zweck bearbeitet. Zudem müssen weitere Modalitäten der Datenbearbeitung wie die Aufbewahrungsdauer der Daten, allfällige Zugriffe Dritter oder der Speicherort der Daten genannt werden. Beim Verfassen einer Datenschutzerklärung ist immer zu beachten, an wen sich diese richtet bzw. wer das Ziel-

publikum der App ist. Nur so kann sichergestellt werden, dass das Zielpublikum die Erklärung versteht und damit gültig in die geplante Datenbearbeitung einwilligt.

Insbesondere bei der Verwendung von Apps erweist sich ein weiterer Grundsatz des Datenschutzrechts, der gerne übersehen wird, als besonders wichtig: Privacy by Default. Darunter versteht man «Datenschutz durch datenschutzfreundliche Voreinstellungen». Dies bedeutet, dass die Werk- bzw. Appeinstellungen datenschutzfreundlich auszugestalten sind. Nach diesem Grundgedanken sollen insbesondere diejenigen Nutzenden geschützt werden, die weniger technikaffin sind und dadurch z. B. nicht geneigt sind, die Einstellungen zum Schutz ihrer Privatsphäre ihren Wünschen entsprechend anzupassen.

Verantwortung der Stadtverwaltung

Bietet die Stadtverwaltung der Bevölkerung eine App an, ist sie dafür verantwortlich, dass die darin enthaltenen Daten korrekt bearbeitet und geschützt werden. Dies gilt insbesondere dann, wenn es um sensible Datenbearbeitungen geht. Die schiere Omnipräsenz von App-Anwendungen und deren einfachen und günstigen Einsatzmöglichkeiten dürfen aber nicht dazu führen, dass unreflektiert mit Personendaten umgegangen wird. Es gilt, bei jeder App, welche angeboten oder von der Verwaltung konzipiert wird, genau zu prüfen, ob die datenschutzrechtlichen Voraussetzungen und Vorgaben eingehalten werden. Bedingung dafür ist, dass auch Apps – und mögen sie noch so unscheinbar sein – als Datenbearbeitungen der Stadtverwaltung erkannt werden, die auf dem städtischem ISDS-Prozess (vgl. Einleitungstext Seite 8) der Datenschutzstelle und dem IT-Security-Team der OIZ zur Prüfung anzumelden sind.

Newsletter der Stadtverwaltung

Der Newsletter ist eine einfache, schnelle und vor allem beliebte Methode, Interessierte über Neuigkeiten zu informieren. Auch die Stadtverwaltung Zürich versendet über 40 verschiedene Newsletter zu diversen Themen an Abonnentinnen und Abonnenten und verschickt somit pro Jahr ungefähr eine Million Newsletter-Mails. Die Stadtverwaltung Zürich verfügt über eine eigene, zentral betriebene Newsletter-IT-Infrastruktur. Rund 90 % der städtischen Newsletter werden über diese Infrastruktur versendet.

Im Berichtsjahr verzeichnete die Datenschutzstelle eine Vielzahl von Anfragen zum Thema Newsletter. Diese kamen einerseits von Privaten, welche sich beispielsweise erkundigten, wo und wie sicher ihre E-Mail-Adressen im Zusammenhang mit einem Newsletter-Abonnement gespeichert sind. Andererseits erkundigten sich aber auch städtische Verwaltungsstellen, ob ihre Einwilligungspraxis datenschutzkonform ausgestaltet ist oder zu welchen konkreten Zwecken sie die E-Mail-Adressen von Newsletter-Kundinnen und -Kunden verwenden dürfen.

Die Datenschutzstelle hat diese Anfragen zum Anlass genommen, die städtische Newsletter-IT-Infrastruktur und den Umgang mit Newslettern in der Stadtverwaltung genauer zu untersuchen. Die aus datenschutzrechtlicher Sicht wichtigsten Punkte zum Thema Newsletter werden nachfolgend dargestellt.

Gültige Einwilligung als Voraussetzung

Wichtigstes Kriterium, damit die Dienstabteilungen der Stadtverwaltung ihre Newsletter versenden dürfen, ist eine konkrete Einwilligung aller Personen, die den Newsletter erhalten sollen. An die gültige Einwilligung der betroffenen Personen werden hohe Anforderungen gestellt. Diese müssen ihre Zustimmung freiwillig, informiert und unmissverständlich in einer eindeutig bestätigenden Handlung abgeben. Eine rein stillschweigende Zustimmung genügt demgegenüber nicht. Die Einwilligung muss beispielsweise mittels Anklicken eines Buttons erfolgen. Zudem muss die Einwilligung jederzeit widerrufen werden können, wobei jeder Newsletter einen deutlichen Hinweis auf die Abmeldemöglichkeit beinhalten muss.

Korrekter Umgang mit Newsletter-Daten in der Verwaltung

Die Dienstabteilungen der Stadtverwaltung, welche Newsletter versenden, müssen die Daten der sich an- und abgemeldeten Personen datenschutzkonform bearbeiten und verwalten. Das heisst konkret, dass die E-Mail-Adressen einzig und allein für den Versand des jeweiligen Newsletters verwendet werden und nicht noch für weitere Zwecke zum Einsatz kommen dürfen. Damit die Dienstabteilungen die An- und Abmeldungen für ihre Newsletter im Griff haben, führen sie regelmässig entsprechende Listen. Auch hier muss die Zweckbindung beachtet werden: Die Liste der abgemeldeten Personen darf nur dazu verwendet werden, sicherzustellen, dass abgemeldete Personen tatsächlich keinen Newsletter mehr erhalten. Über diesen Kontrollzweck hinaus dürfen die E-Mail-Adressen der abgemeldeten Personen nicht verwendet werden, insbesondere auch nicht dafür, eine gewisse Zeit nach der Abmeldung die abgemeldeten Personen anzufragen, ob sie wieder Interesse am Newsletter hätten.

Und die europäische DSGVO?

Die im Frühjahr 2018 in Kraft getretene europäische Datenschutzgrundverordnung (DSGVO) sorgte in der Schweiz für grosse Aufregung und beeinflusste unter anderem das Vorgehen beim Newsletter-Marketing enorm. Was verlangt nun aber die DSGVO im Bereich Newsletter eigentlich und genügt die Stadtverwaltung mit ihrer Einwilligungspraxis derselben? Die Datenschutzstelle hat diese Frage geklärt und wiederholt beantwortet, obwohl die DSGVO für die Stadtverwaltung grundsätzlich keine Geltung hat.

Damit der Versand eines Newsletters DSGVO-konform ist, muss der Empfänger dem Empfang explizit zugestimmt haben, d. h. die Einwilligung darf nicht Teil einer formulierten Vertragsbedingung und das erforderliche Zustimmungs-Häkchen auf keinen Fall automatisch gesetzt sein. Mehrheitlich wird die Einwilligung mit dem sogenannten Double-Opt-In-Verfahren abgeschlossen. Bei diesem Verfahren erhält ein neuer Newsletter-Abonnent eine automatische E-Mail, um die eingetragene E-Mail-Adresse sowie das Erteilen der Zustimmung zum Versenden von Newslettern (nochmals) zu bestätigen. Beim Double-Opt-In-Verfahren handelt es sich zwar um eine verbreitete Praxis, um eine rechtliche Anforderung der DSGVO handelt es sich aber nicht.

Die Stadtverwaltung verzichtet denn auch auf diese doppelte Bestätigung der Newsletter-Einwilligung. Mit ihrer Einwilligungspraxis, der jederzeitigen Abmeldemöglichkeit sowie dem datenschutzkonformen Umgang mit den Newsletter-Daten im Sinne der Einhaltung der Zweckbestimmung erfüllt die Stadtverwaltung nicht nur die Anforderungen des für sie geltenden IDG. Auch die Anforderungen der DSGVO, die wie erwähnt nur in Ausnahmefällen überhaupt zur Anwendung kommen kann, würde sie damit erfüllen.

E-Governance und Newsletter

Die Nutzung der städtischen Newsletter-IT-Infrastruktur durch eine Dienstabteilung bietet aus der Sicht der Newsletter-Abonnentinnen und -Abonnenten einen weiteren entscheidenden Vorteil: Ihre Daten bleiben auf dem städtischen Server und werden nicht weitergegeben. Dies ist anders, wenn eine Dienstabteilung einen privaten Newsletter-Dienst nutzt. In diesem Fall werden die Daten der Newsletter-Abonnenten oft an private Newsletter-Dienstanbieter weitergegeben und regelmässig auf ausländischen Servern gespeichert.

Die städtische Newsletter-IT-Infrastruktur ist seit 2018 an das E-Government-Portal der Stadt Zürich («Mein Konto») gekoppelt. Jede Person, die sich für einen städtischen Newsletter anmeldet, muss sich auch für einen «Mein Konto»-Account registrieren. Diese Registrierung bringt mit sich, dass neben der Email-Adresse und dem Namen der Person auch weitere Daten abgefragt werden und ein Passwort erstellt werden muss. Beim Registrierungsprozess sind zwar viele der gefragten Daten wie Adresse oder Telefonnummer nicht zwingend, dennoch werden diese wohl von vielen Personen wahrheitsgemäss ausgefüllt. Aus datenschutzrechtlicher Sicht stellt sich im Zusammenhang mit diesem Vorgehen die Frage, ob durch das Abfragen von diesem «Zu Viel» an Daten das Prinzip der Datensparsamkeit sowie der Verhältnismässigkeit verletzt wird. Diese Prinzipien besagen, dass nur so viele Daten erhoben werden sollen, wie zur Erfüllung des Zwecks unbedingt nötig sind. Zur Versendung bzw. Registrierung eines Newsletters bedarf es nur der Angabe einer Email-Adresse und keiner weiteren Daten. Die Datenschutzstelle hat diese Frage als Prüfpunkt in die pendente Erarbeitung von E-Governance-Grundlagen der Stadt Zürich eingebracht.

FOKUS 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.

Bei der Datenschutzstelle melden sich immer wieder städtische Angestellte mit Fragen oder Beschwerden zum Datenschutz im Personalbereich. Eines der zentralen Anliegen betrifft die Überwachung am Arbeitsplatz. Die zunehmende Technologisierung zahlreicher Arbeitsplätze erhöht die Möglichkeit, auch das Verhalten oder die Leistung der Angestellten auswerten oder überwachen zu können. Nebst Fragen nach Zulässigkeit und Verhältnismässigkeit allfälliger Auswertungen oder Überwachungen sind es vor allem auch die Transparenz- und Informationsmassnahmen gegenüber den Angestellten, die Gegenstand von Beratungen und Prüfungen durch die Datenschutzstelle sind.

In personalrechtlichen Verhältnissen müssen oft auch sehr vertrauliche und sensitive Gesundheitsdaten bearbeitet werden, so z. B. im Case Management oder bei vertrauensärztlichen Abklärungen.

Auch solche Belange führen regelmässig zu Anfragen bei der Datenschutzstelle.

Die beiden nachfolgenden Beispiele aus dem Berichtsjahr betreffen weitere Belange im Personalbereich und unterstreichen damit die grosse Bandbreite datenschutzrechtlicher Fragestellungen in diesem Kontext.

Plattform für Online-Bewerbung

Die Stadt Zürich ist eine attraktive und moderne Arbeitgeberin. Damit sie dies auch in Zukunft bleibt, muss sie über ein zeitgemässes Bewerbungsmanagement verfügen. Im Berichtsjahr lancierte die Dienstabteilung Human Resources Management (HRZ) eine städtische Plattform, auf welcher die Verwaltungsstellen der Stadt Zürich ihre Stellen ausschreiben und interessierte Personen ihre Bewerbungen einreichen können. Mit dem städtischen Personalrecht sind gesetzliche Grundlagen zu Bewerbung und Umgang mit Bewerbungsinformationen vorhanden. Da diese nicht nur bei Papier-, sondern auch bei elektronischen Bewerbungen gelten, schienen sich die datenschutzrechtlichen Themen bei diesem Vorhaben vor allem auf die Informationssicherheit und die Zugriffsregelung zu fokussieren. Doch wie so oft zeigte sich auch hier, dass der Teufel bzw. die datenschutzrechtliche Herausforderung im Detail liegen kann.

Wer sich über die neue Plattform für eine Stelle bei der Stadt Zürich bewerben will, hat hierfür ein Benutzerkonto zu eröffnen, in welchem sogenannte Profilinformationen zu hinterlegen sind. Dazu gehören nebst Angaben zu Namen, Anschrift, E-Mail-Adresse und Telefonnummer auch die üblichen Bewerbungsunterlagen (Lebenslauf, Diplome, Zeugnisse und dgl.). Im Rahmen der Eröffnung des Benutzerkontos müssen sich die Bewerberinnen und Bewerber entscheiden, für wen ihre Profilinformationen zugänglich sein sollen. Sie haben die Wahl zwischen der (offenen) Einsehbarkeit für alle RecruiterInnen der Stadt Zürich (Option 1) oder einer (eingeschränkten) Einsehbarkeit nur für diejenigen RecruiterInnen, die die Stelle betreuen, auf die sie sich konkret bewerben (Option 2). Während sich die Möglichkeit zur Einsichtnahme in die Profilinformationen bei Option 2 auf wenige Personen beschränkt, sind bei Option 1 die Informationen mehreren hundert städtischen HR-Fachpersonen der Rekrutierungsstellen

zugänglich. Eine solche Bewerbungsmöglichkeit, die quasi die gesamte Stadtverwaltung adressiert, kann durchaus im Interesse von Bewerbenden sein. Für sie muss jedoch die Tragweite dieser Bewerbungsoption klar erkennbar und verständlich sein, insbesondere weil Profilinformationen in aller Regel vertraulich sind und sensitive Personendaten enthalten. Die Datenschutzstelle stellte deshalb erhöhte Anforderungen an die Transparenz und Information. Die Bewerberinnen und Bewerber sind nicht nur klar und umfassend, sondern vor allem auch rechtzeitig, d. h. bereits bei der Eröffnung eines Benutzerkontos und somit unmittelbar bei der Wahl der Optionen, entsprechend zu informieren. Dabei ist auch zu berücksichtigen, dass für Aussenstehende die städtischen Zuständigkeiten in HR-Belangen nicht ohne Weiteres bekannt sind.

Das städtische Personalrecht verlangt, dass Bewerbungsinformationen bei Nichtanstellung zu vernichten sind, sofern die Bewerbenden nicht einer weiteren Aufbewahrung zustimmen. Die Umsetzung dieser an sich unbestrittenen Forderung aus dem Personal- und Datenschutzrecht erweist sich im vorliegenden Projekt als weitere Herausforderung. Eine zu rasche oder kategorische Löschung der Daten nach Abschluss von Bewerbungsverfahren kann sich als nicht adäquat oder gar kontraproduktiv erweisen. Berechtigte Interessen an einer weiteren Verfügbarkeit können sowohl auf Seiten der Stadt als Arbeitgeberin als auch auf Seiten der Bewerbenden bestehen. Zu klären gilt es deshalb erst einmal, wie lange Bewerbungsunterlagen von nicht berücksichtigten Kandidatinnen und Kandidaten oder bei Rückzug durch die Bewerbenden mit Zustimmung der Betroffenen weiterhin gespeichert bleiben sollen. In direktem Zusammenhang mit dieser Klärung stellt sich die weitere Frage, wie die verlangte Zustimmung der Bewerbenden für die weitere Aufbewahrung erteilt werden muss. Eine Zustimmung kann entweder in Form einer ausdrücklichen Zustimmung (opt-in) oder als Unterlassung eines möglichen Wider-

spruchs (opt-out) erfolgen. Weder das kantonale Datenschutzrecht noch das städtische Personalrecht enthalten in Bezug auf die Zustimmungserfordernisse Vorgaben. Auszugehen ist deshalb vom allgemeinen Grundsatz, wonach sich die Anforderungen an eine Zustimmungserklärung bzw. Einwilligung nach der Sensitivität der Daten zu richten haben. Nach Ansicht der Datenschutzstelle muss zwar selbst bei Personaldaten, die vertraulich und sensitiv sein können, eine opt-out-Lösung nicht grundsätzlich ausgeschlossen werden. Voraussetzung ist jedoch, dass die vorgesehene Aufbewahrungsdauer sachgerecht und zurückhaltend festgelegt ist und dass die Plattform so konzipiert ist, dass die Benutzenden ihre Informationen jederzeit und auf leicht zugängliche Weise löschen können.

Projektleitung und Datenschutzstelle konnten sowohl hinsichtlich Transparenz und Information als auch hinsichtlich Löschung und Zustimmung noch keine abschliessende Einigung erzielen. Die Prüfung der Datenschutzstelle konnte deshalb noch nicht abgeschlossen werden.

Angaben über Angestellte der Stadtverwaltung

Im Berichtsjahr wurde die Datenschutzstelle wiederholt mit der Frage konfrontiert, ob im Rahmen von Auskunftsgesuchen auch Personendaten von Verwaltungsangestellten bekanntgegeben werden müssen.

Jede Person kann gestützt auf das Datenschutzrecht Auskunft darüber erhalten, welche Personendaten eine Verwaltungsstelle über sie bearbeitet. Ausserdem besteht gestützt auf das Öffentlichkeitsprinzip ein Anspruch auf Zugang zu (weiteren) Informationen der Stadtverwaltung. Das angefragte öffentliche Organ ist verpflichtet, entsprechende Gesuche zu behandeln und über die bearbeiteten Daten Auskunft zu erteilen. Nun gelten diese Rechte auf Auskunft aber nicht absolut, so dass in begründeten Ausnahmefällen gewisse Daten von der Herausgabe ausgenommen bzw. geschwärzt werden können.

Dies ist dann erlaubt, wenn ein höheres privates oder öffentliches Interesse gegen eine Herausgabe spricht. Im Normalfall enthalten Daten, welche die Verwaltung bearbeitet, auch die Namen der involvierten Mitarbeitenden der Verwaltung. Müssen diese Mitarbeitendendaten vor der Herausgabe an die gesuchstellende Person geschwärzt werden? Darf beispielsweise die Polizei bei der Herausgabe von Berichten die Namen involvierter Polizistinnen und Polizisten abdecken? Oder darf der Stadtärztliche Dienst die Namen der mit dem Fall befassten Ärztinnen und Ärzte aus seinen Berichten streichen?

Die Antwort lautet: Nein, im Normalfall nicht. Denn gemäss Rechtsprechung ist davon auszugehen, dass sich Verwaltungsangestellte mit Blick auf die Erfüllung ihrer öffentlichen Aufgaben grundsätzlich nicht im selben Mass auf ihr Recht auf informationelle Selbstbestimmung berufen können wie Privatpersonen. Ihren privaten Interessen, die einem Zugang bzw. einer Auskunft entgegenstehen können, kommt grundsätzlich weniger Gewicht zu, als wenn Personendaten privater Dritter in Frage stehen. Dabei muss jedoch unterschieden bzw. differenziert werden: Je höher die Funktionsstufe, desto weitergehende Eingriffe in die Persönlichkeitssphäre können zulässig sein. Verwaltungsangestellte in hohen Führungsfunktionen müssen sich unter Umständen sogar die Bekanntgabe besonders schützenswerter Personendaten gefallen lassen. Bei hierarchisch nachgeordneten Verwaltungsangestellten wird dies kaum je der Fall sein. Diese müssen aber grundsätzlich damit rechnen, dass bekannt wird, wer beispielsweise in amtlicher Funktion wie gehandelt oder eine bestimmte Meinung vertreten hat bzw. wer ein bestimmtes Dokument verfasst hat oder für ein bestimmtes Geschäft zuständig war. Die Bekanntgabe von Personendaten steht jedoch in jedem Fall unter dem Vorbehalt überwiegender Nachteile für die betroffenen Verwaltungsangestellten. Die Nachteile müssen dabei von einigem Gewicht sein; geringfügige oder bloss unangenehme Konsequenzen reichen nicht aus!

Zusammenfassend kann gesagt werden, dass bei Auskunftsgesuchen Daten von Mitarbeitenden, die sich auf dienstliche Funktionen bzw. deren Erfüllung beziehen, grundsätzlich herausgegeben werden müssen. Nur im Ausnahmefall, bei Vorliegen konkreter, im Einzelfall zu prüfender Gründe, können diese geschwärzt werden. Dabei gilt es zu beachten, dass die Verwaltung bei Einschränkung der Bekanntgabe von Mitarbeitendendaten durch Schwärzung oder Abdeckung – so wie bei jeder Einschränkung von Auskunftsgesuchen – eine begründete und beschwerdefähige Verfügung erlassen muss.

FOKUS 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 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. Unter Rohdaten werden alle Daten verstanden, 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 üblicherweise 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.

Datenanalysen

Die Stadtverwaltung ist verpflichtet, ihre Ressourcen und finanziellen Mittel rechtmässig, wirksam und effizient einzusetzen. Für die Planung und Kontrolle des Ressourceneinsatzes spielen Datenanalysen eine wichtige Rolle. Hierfür werden bereits bestehende Daten ausgewertet. Ergebnis solcher Auswertungen sind vorwiegend statistische Werte ohne Aussagekraft auf Einzelpersonen. Bisher definieren Dienstabteilungen, Departemente und Behörden selber, welche konkreten Auswertungen sie als notwendig erachten und welche Daten hierfür verwendet werden sollen. Die Auswertungen erfolgen bis heute in der Regel direkt über die Fachapplikationen der jeweiligen Dienstabteilungen und sind je nach deren Technologien und Funktionalitäten mehr oder weniger aussagekräftig.

In den letzten Jahren sind neue Analysetechnologien internationaler Anbieter wie SAP, Microsoft oder Amazon auf den Markt gekommen, welche die Möglichkeiten herkömmlicher Datenanalysen zum Teil revolutionieren. Mit Hilfe von Künstlicher Intelligenz und sogenanntem «machine learning» können riesige Mengen an Daten zum Teil sogar in Echtzeit analysiert und ausgewertet und die Ergebnisse visualisiert werden. Die Datenanalysesysteme enthalten fast unzählige vorprogrammierte Einzelkomponenten, mit welchen quasi auf Knopfdruck die entsprechenden Analysen ausgelöst werden können.

Die neuen Analysetechnologien haben mittlerweile auch Einzug in die Stadtverwaltung gehalten. Allerdings steht man erst am Anfang: In einzelnen Fachbereichen will man in Form von Pilotvorhaben erste Erfahrungen sammeln und insbesondere prüfen, welche Analysekomponenten sinnvoll genutzt werden können. Dies bedingt, dass bereits während den Pilotphasen die Analysekomponenten produktiv eingesetzt und hierfür die notwendigen Personendaten bereitgestellt

werden. Für die Datenschutzstelle ist nachvollziehbar, dass derartige neue Technologien und Möglichkeiten auch für den Verwaltungsbereich evaluiert und getestet werden und dass die Stadtverwaltung hierfür über einen gewissen Spielraum verfügen muss. Allerdings müssen die Grenzen so gezogen werden, dass die geltenden datenschutzrechtlichen Bestimmungen eingehalten werden.

Da im Rahmen der einzelnen Pilotvorhaben die Bearbeitungszwecke und die mit der Nutzung der Analysetechnologien verbunden Risiken noch nicht abschliessend bekannt sind, hat die Datenschutzstelle verlangt, dass Personendaten ausschliesslich zu nicht personenbezogenen Zwecken und damit nur anonymisiert und somit ohne Rückschlussmöglichkeiten auf Einzelpersonen ausgewertet werden dürfen. Auch hat die Datenschutzstelle verlangt, dass vorerst keine sensiblen Personendaten bearbeitet werden, denn solche Daten, beispielsweise aus dem Polizei-, Sozialhilfe- oder Gesundheitsbereich, bergen unabhängig vom Bearbeitungszweck ein erhöhtes Risiko für Persönlichkeitsverletzungen in sich.

Bereits heute ist davon auszugehen, dass nach Abschluss der einzelnen Pilotvorhaben die neuen Analysetechnologien definitiv eingesetzt werden und dabei die Dienstabteilungen wohl auch personenbezogene Analysen durchführen und generell für ihre Analysen auch sensible Personendaten verwenden werden. Die Datenschutzstelle erachtet es daher als wichtig, dass frühzeitig in der Stadtverwaltung die richtigen Weichen für die datenschutzkonforme Nutzung solcher Technologien gestellt werden. In einem ersten Schritt hat die Datenschutzstelle die Durchführung einer Risikofolgeabschätzung verlangt. Ob eine solche generisch erfolgen kann oder für jede einzelne fachbereichsspezifische Analyse verlangt werden muss, werden die weiteren Abklärungen zeigen.

Datenschutzkonzepte

Die Stadtverwaltung verfügt über grosse Mengen an sensiblen Personendaten. Diese Daten sind nicht nur für die verwaltungsinterne Forschung, Planung und Statistik von grossem Interesse, sie werden auch von externen Forschungsstellen (Hochschulen, Universitäten) regelmässig bei der Stadtverwaltung nachgefragt. Die Bekanntgabe solcher Daten ist mit einem erhöhten Risiko für die Persönlichkeit und die Privatsphäre der betroffenen Personen verbunden. Die städtische Datenschutzverordnung verlangt deshalb, dass solche Bekanntgaben – und zwar sowohl interne Bekanntgaben unter den Dienstabteilungen als auch Datenbekanntgaben gegenüber externen Stellen – im Rahmen von Vorabkontrollen durch die Datenschutzstelle geprüft werden. Ebenfalls durch die Datenschutzstelle zu prüfen sind Forschungs-, Planungs- und Statistikvorhaben, bei welchen sensible Personendaten durch die Stadtverwaltung beispielsweise mittels Umfragen oder Interviews direkt bei den Bürgerinnen und Bürger erhoben werden.

Regelmässig beinhalten Forschungsvorhaben sowohl Datenbekanntgaben als auch Direkterhebungen. Als Beispiel aus dem Berichtsjahr sei etwa ein Nationalfondprojekt erwähnt, welches sich mit der Fürsorgepraxis bei Kindervernachlässigung befasste und hierfür Einsicht in sensible Akten der KESB benötigte und auch die Durchführung von Interviews bei Fachpersonen und bei betroffenen Müttern vorsah.

Das Datenschutzrecht verlangt bei Datenbekanntgaben von den Forschungs-, Planungs- und Statistikstellen, dass sie die benötigten Personendaten, den Ablauf der Datenbearbeitung und die Schutzmassnahmen in einem schriftlichen Gesuch darlegen. Betrifft ein solches Gesuch sensible Personendaten, gelten erhöhte Anforderungen an die Schutzmassnahmen. Gleiches gilt in Bezug auf die

Schutzmassnahmen bei sensiblen Direkterhebungen. Anders als bei IT-Projekten besteht bei Bekanntgaben und Direkterhebungen zu nicht personenbezogenen Zwecken kein Standard und keine Best Practice, die zur Ausarbeitung eines Datenschutzkonzeptes verpflichten würden. Trotzdem erachtet es die Datenschutzstelle als wichtig und notwendig, dass auch bei solchen Vorhaben ein Datenschutzkonzept verfasst wird. Denn nur ein solches Konzept bietet Gewähr, dass die Datenschutzanforderungen wie insbesondere die erforderlichen Schutzmassnahmen vollständig, nachvollziehbar und kontrollierbar geregelt werden.

Regelmässiger Gegenstand eines Datenschutzkonzeptes sind die folgenden Datenschutzthemen:

– Verantwortlichkeiten: An der Durchführung von Forschungs-, Planungs- und Statistikvorhaben sind oft mehrere Stellen beteiligt. Es muss klar sein, wer in welcher Rolle für die einzelnen Datenbearbeitungsprozesse verantwortlich ist.

– Anonymisierung auf Ebene Rohdaten: Die gesetzlich verlangte Datenanonymisierung ist in der Praxis oft ein schwieriges Unterfangen. Scheinbar anonymisierte Daten können bei näherer Betrachtung Rückschlussmöglichkeiten auf Einzelpersonen geben. Solche können sich insbesondere aus demographischen (z. B. Alter, Geschlecht, Beruf) oder örtlichen Angaben (z. B. Wohnort, Geo-Koordinaten) sowie insbesondere aus Kombinationen und Verknüpfungen der verwendeten Attribute ergeben. Solche Rückschlussmöglichkeiten müssen soweit und sobald als möglich verhindert werden.

– Anonymisierung auf Ebene Auswertungen: Gestützt auf das Datenschutzrecht dürfen spätestens bei den Auswertungen keine Rückschlussmöglichkeiten auf Einzelpersonen mehr möglich sein. In der Praxis geschieht dies regelmässig durch die Aggregation (Zusammenfassung) der Daten. Dies kann zu einem Interessenkonflikt zwischen den Zielen eines Vorhabens und dem Datenschutz führen: Je weiter die Aggregation der Daten erfolgt (beispielsweise räumliche Datenauswertungen auf Ebene Quartier anstatt Wohnadresse), desto unspezifischer werden die Auswertungsergebnisse. Für eine datenschutzrechtliche Beurteilung müssen bei der Aggregation der Daten die Risiken für eine allfällige Deanonymisierung miteinbezogen werden. Die Risikobeurteilung hängt insbesondere davon ab, für welche Zwecke die Auswertungen zur Verfügung stehen. Erhöhte Risiken ergeben sich insbesondere bei Veröffentlichungen, da bei diesen jegliche Kontrollmöglichkeiten über die Weiterverwendung aus der Hand gegeben werden.

– Löschungsfristen: Das Datenschutzrecht verlangt, dass die Personendaten gelöscht werden, sobald der Bearbeitungszweck erreicht ist, spätestens jedoch nach Abschluss der Auswertungen. In der Praxis zeigt sich oft, dass die Löschung der Daten nicht nur in einem einzigen Schritt erfolgen kann, so dass Löschungsfristen für Teilprozesse der Datenbearbeitungen definiert werden müssen.

– Informationssicherheit: Wie bei allen Vorhaben, bei welchen Personendaten bearbeitet werden, müssen auch bei Forschungs-, Planungs- und Statistikvorhaben die sicherheitstechnischen Anforderungen erfüllt werden. Dabei geht es beispielsweise um die Verschlüsselung der Datenübermittlung, das Berechtigungskonzept sowie – insbesondere beim Einsatz von Datenbearbei-

tungssystemen ausserhalb der städtischen Informatikinfrastruktur – um den Nachweis weiterer technischer und organisatorischer Schutzmassnahmen (z. B. Angaben zur Zertifizierung).

– Einverständniserklärung bei direkten Erhebungen: Eine rechtsgültige Einverständniserklärung setzt eine ausreichende Aufklärung voraus. Nur wer ausreichend aufgeklärt ist, kann einen fundierten und freien Entscheid über die Preisgabe seiner Daten fällen. Die betroffenen Personen sollen verstehen, zu welchem Zweck die Daten benötigt werden, wie und durch wen die Daten bearbeitet werden und ob und wie die Anonymisierung der Daten gewährleistet wird. Liegt ein Abhängigkeitsverhältnis vor – wie dies beispielsweise im Sozial-, Medizin- oder Schulbereich der Fall sein kann – erachtet es die Datenschutzstelle als wichtig, dass die Betroffenen ausdrücklich darauf hingewiesen werden, dass ihnen bei einer Nicht-Teilnahme keine Nachteile erwachsen dürfen und sie auch bei einer Teilnahme jederzeit den Rücktritt erklären können. Die Einräumung einer Bedenkfrist kann die Betroffenen in ihrer freien Entscheidungsfindung unterstützen.

Dienstabteilungen sind in der Praxis oft unsicher, ob ein Forschungs-, Planungs- oder Statistikvorhaben in einem sensiblen Bereich überhaupt zulässig ist. Ein durch die Datenschutzstelle geprüftes Datenschutzkonzept ist für sie eine wichtige Entscheidungsgrundlage und schafft Klarheit bezüglich der konkreten Datenbearbeitungsprozesse. Für die hinter den Daten stehenden Einzelpersonen bietet das Datenschutzkonzept und die Prüfung durch die Datenschutzstelle Gewähr, dass der Schutz ihrer Persönlichkeit und Privatsphäre auch bei Forschungs-, Planungs- und Statistikvorhaben ernst genommen wird.

FOKUS
OPEN GOVERNMENT DATA

Die Verwaltung verfügt über umfangreiche und qualitativ hochstehende Informationen und Daten. Diese für interessierte Unternehmen und Privatpersonen soweit wie möglich zugänglich zu machen, ist das Ziel von Open Government Data (OGD). Demnach sollen Datenbestände der Verwaltung, die kein Schutzbedürfnis haben, allen Interessierten in maschinenlesbarer Form frei von Nutzungseinschränkungen verfügbar gemacht werden. OGD soll Transparenz, Partizipation und Innovation in allen gesellschaftlichen Bereichen fördern und helfen, Verwaltungshandeln durch Vereinfachung der Datennutzung über organisatorische und systemische Grenzen hinweg effektiver zu gestalten. Die als OGD veröffentlichten Datensätze werden als offene Verwaltungsdaten bezeichnet. Sie werden auf spezifischen OGD-Portalen veröffentlicht und so allen Interessierten zugänglich gemacht. In der Schweiz bestehen OGD-Portale auf allen Staatsebenen. Bis anhin sind es vor allem Geo-, Statistik- oder Messdaten, die auf den OGD-Portalen der Verwaltungen in maschinenlesbarer Form zur freien Nutzung publiziert werden.

Im Kontext von OGD wird dem Datenschutz regelmässig hohe Bedeutung zugesprochen. Das verwundert nicht, denn OGD kann nur funktionieren, wenn veröffentlichte Daten den Schutz von Persönlichkeit und Privatsphäre gewährleisten. Datenschutz ist somit auch bei OGD Vertrauensbasis. Um den Persönlichkeitsschutz bei OGD zu gewährleisten, genügen jedoch bloss allgemeine Bekenntnisse zum Datenschutz nicht. Die Sicherstellung, dass offene Verwaltungsdaten keinen Personenbezug haben, dass bei anonymisierten Daten keine Re-Identifikation möglich ist oder dass auch bei Verknüpfung mit

anderen Daten Persönlichkeitsverletzungen ausgeschlossen werden, erfordert konkrete und verbindliche Massnahmen. Im Vordergrund stehen vor allem Anonymisierungsverfahren. Herausforderung dabei ist auch der Umgang mit dem Zielkonflikt, wonach mit zunehmendem Aggregationslevel, das heisst mit zunehmender Zusammenfassung und Abstrahierung von Werten (beispielswiese auf Quartiere anstelle von einzelnen Liegenschaften) zwar der Persönlichkeitsschutz besser gewährleistet, gleichzeitig aber auch die Nutzbarkeit und somit der Wert der Daten verringert wird.

Welche Anforderungen Datensätze für OGD-Tauglichkeit zu erfüllen haben, wird noch weitgehend durch Standards und Best Practices definiert. Rechtliche Regelungen für OGD bestehen kaum. Beim Bund gilt die «OGD-Strategie 2019 – 2023». Sie beinhaltet insbesondere den für die Bundesverwaltung verbindlichen Grundsatz, wonach öffentliche Daten unter Vorbehalt entgegenstehender rechtlicher Vorschriften grundsätzlich und soweit technisch möglich von den Dateneignern in maschinenlesbarer Form publiziert werden sollen. Im Rahmen dieser Strategie wird der Bund prüfen, ob mit einem Rechtsetzungsvorhaben OGD-Grundsätze rechtlich verankert werden sollen. Auch der Kanton Zürich verfügt über keine spezialgesetzlichen Grundlagen zu OGD. Auf kantonaler Ebene ist OGD Gegenstand der Strategie «Digitale Verwaltung».

Für die Stadt Zürich hat der Stadtrat erstmals 2012 eine OGD-Strategie sowie eine OGD-Richtlinie erlassen und in der Amtlichen Rechtsammlung publiziert. Die offenen Verwaltungsdaten der Stadt Zürich werden Interessierten auf dem städtischen OGD-Portal (data.stadt-zuerich.ch) zur Verfügung gestellt. Stand April 2020 sind es 562 Datensätze.

Revision der städtischen OGD-Grundlagen

Bereits 2018 hat der Stadtrat mit der Strategie «Smart City Zürich» die Wichtigkeit offener Verwaltungsdaten als Basisinfrastruktur einer digitalen und vernetzten Stadt unterstrichen und für die Weiterentwicklung des städtischen OGD den Grundsatz «Open by Default» eingeführt. Mit der Revision der OGD-Strategie soll dies nun konkretisiert werden. Anstelle der bisherigen OGD-Richtlinien sollen neu OGD-Leitlinien und -Prozesse definiert werden. Im Berichtsjahr äusserte sich die Datenschutzstelle zur Revision dieser städtischen OGD-Grundlagen.

Aus datenschutzrechtlicher Sicht ist im Kontext von OGD in erster Linie zu verlangen, dass offene Verwaltungsdaten keine Personendaten im Sinne der Datenschutzgesetzgebung beinhalten. Ausnahmen von diesem Grundsatz können sich allenfalls aus bereichsspezifischen Rechtsgrundlagen wie insbesondere der Geoinformationsgesetzgebung ergeben. Aufgabe der verantwortlichen Verwaltungseinheiten ist somit, ihre Datensätze dahingehend zu prüfen, ob sie Personendaten beinhalten und wie gegebenenfalls deren Personenbezug eliminiert werden kann. Beide Prüfschritte – sowohl das Erkennen von Personendaten als auch deren Eliminierung – können unter Umständen sehr anspruchsvoll sein und ohne spezifische Kompetenzen nicht durchgeführt werden. So verlangen insbesondere Anonymisierungsverfahren besondere Methodenkompetenzen und technisches Spezialwissen. Für die Gewährleistung von Persönlichkeits- und Datenschutz werden qualifiziertes Know-how, interdisziplinäre Zusammenarbeit sowie genügende Ressourcen unabdingbar sein. Dies umso mehr, als mit dem Grundsatz «Open by Default» künftig nicht nur Sachdaten, sondern vermehrt auch datenschutzrechtlich relevante Verwaltungsdaten auf OGD-Tauglichkeit hin zu überprüfen sein werden. Erreicht werden kann dies nur mit der Etablierung verbindlicher, systematischer und institutionalisierter Prüfverfahren.

Die Revisionsvorlage sieht vor, dass die erforderlichen Prüfungen der Verwaltungsdaten auf OGD-Tauglichkeit durch die über 60 Verwaltungseinheiten der Stadt Zürich (Departemente, Dienstabteilungen und Fachstellen), welche originär für die Daten verantwortlich sind, vorgenommen werden. Nach Einschätzung der Datenschutzstelle werden viele der städtischen Verwaltungsstellen ohne Unterstützung dazu weder fachlich noch mit den zur Verfügung stehenden Ressourcen in der Lage sein. Die Datenschutzstelle hat deshalb in ihrer Stellungnahme vorgeschlagen zu prüfen, ob die Stadt Zürich für das städtische OGD ein Kompetenzzentrum einsetzen kann. Diesem sollte nicht nur Beratungs- und Supportaufgaben zukommen, sondern beispielsweise auch die Gewährleistung des erforderlichen Know-hows sowie die Etablierung von Prüf- und Anonymisierungsverfahren, wozu insbesondere auch der technische Datenschutz gehören muss.

In ihrer Stellungnahme verwies die Datenschutzstelle auch darauf, dass sich bei OGD vermehrt Fragen stellen, die über den Datenschutz hinausgehen, insbesondere jene der Gefahr von Diskriminierung oder Stigmatisierung von Bevölkerungsgruppen (beispielsweise bei Informationen über kleinräumige Verhältnisse wie Strassen oder Siedlungen). Es ist daher wichtig, dass Verwaltungsdaten im Hinblick auf OGD-Tauglichkeit nicht nur mit Blick auf den Datenschutz geprüft, sondern mit offener Sichtweise regelmässigen und umfassenden Risikoanalysen unterzogen werden.

FOKUS VIDEOÜBERWACHUNG

Die Stadt Zürich hat für Videoüberwachungen 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.

Die Beratungen zum Thema Videoüberwachung und die Prüfungen von Videoreglementen beanspruchen die Datenschutzstelle in besonderem Masse. Eine Übersicht über den Stand der Videoüberwachung durch die Stadtverwaltung folgt gleich anschliessend.

Beratungen und Prüfungen

Die Datenschutzverordnung der Stadt Zürich verpflichtet die Stadtverwaltung, für Videoüberwachungen mit Aufzeichnung Reglemente zu erstellen. In den neun Jahren, seit die Datenschutzverordnung in Kraft ist, haben mehrere 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 technisches Know-how über die jeweilige Videoanlage sowie 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.

Übersicht über städtische Videoreglemente

Aktuell haben 13 städtische Dienstabteilungen Videoüberwachungen gestützt auf die Datenschutzverordnung der Stadt Zürich im Einsatz. Entsprechende Reglemente haben die Dienstabteilungen Stadtpolizei, Organisation und Informatik, Stadtspitäler Triemli und Waid, Städtische Gesundheitsdienste, Immobilien, Liegenschaften, Sportamt, Museum Rietberg, Wasserversorgung, Entsorgung + Recycling, Tiefbauamt und Elektrizitätswerk erlassen. Abrufbar sind die Reglemente in der Amtlichen Sammlung der Stadt Zürich (bis auf wenige Ausnahmen, deren Aufnahme in die Amtliche Sammlung bald erfolgen wird).

Auswirkungen des revidierten Gemeindegesetzes

Am 1. Januar 2018 trat das revidierte Gemeindegesetz des Kantons Zürich in Kraft. Eine der nun zwischenzeitlich festgestellten Konsequenzen dieser Revision betrifft die Zuständigkeit für den Erlass von Videoreglementen gemäss städtischer Datenschutzverordnung. Bis anhin waren es die Dienstchefs oder Dienstchefinnen, die die Videoreglemente erlassen haben. Mit der Revision des Gemeindegesetzes liegt diese Zuständigkeit nun zwingend bei den Departementsvorstehern oder Departementsvorsteherinnen. Videoreglemente, die nach dem 1. Januar 2018 (fälschlicherweise) noch durch die Dienstabteilungen erlassen wurden, müssen entsprechend der neuen Zuständigkeitsregelung neu erlassen werden.

Anfragen Privater

Im Berichtsjahr meldeten sich rund 20 Privatpersonen bei der Datenschutzstelle mit Fragen oder Anliegen zu Videoüberwachung. Wie bereits im Vorjahr betrafen sämtliche Anfragen von Privatpersonen Videoüberwachungen, für die nicht die Stadtverwaltung, sondern Private zuständig waren. Von den fraglichen Videoüberwachungen war in vielen Fällen auch öffentlicher Grund der Stadt Zürich (mit-) betroffen.

Für Videoüberwachungen durch Private sind die privatrechtlichen Bestimmungen des Bundesgesetzes über den Datenschutz massgebend. Die Vorschriften des kantonalen Datenschutzgesetzes oder der städtischen Datenschutzverordnung kommen in diesen Fällen nicht zur Anwendung, da Private für die Videoüberwachung verantwortlich sind. Zuständig für Beratung und Aufsicht bei Videoüberwachung durch Private ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB). Sofern Anfragen von Privaten bloss mit einer allgemeinen Rechtsauskunft beantwortet werden konnten, erteilte die städtische Datenschutzstelle dennoch gerne Auskunft. Bei allen übrigen Anfragen verwies die Datenschutzstelle die anfragenden Personen wie bereits in den vergangenen Jahren aus Zuständigkeitsgründen an den EDÖB weiter.

Neue Zuständigkeit der Datenschutzstelle

Die Zuständigkeit für Beratungen im Bereich privater Videoüberwachungen könnte sich in der Stadt Zürich bald ändern. Die Motion GR Nr. 2017/63 verlangt, dass die Beratungsaufgaben der Datenschutzstelle erweitert werden. Künftig soll die Datenschutzstelle auch Anfragen zu Videoüberwachung durch Private beantworten, sofern diese Videoüberwachungen öffentlichen Grund der Stadt Zürich tangieren.

Im Berichtsjahr hat der Stadtrat zur Umsetzung dieser Motion vorgeschlagen, in der Datenschutzverordnung eine entsprechende Beratungs- und Vermittlungskompetenz der oder des städtischen Datenschutzbeauftragten vorzusehen. Ausschlaggebend wäre in jedem Fall, dass der öffentliche oder allgemein zugängliche Raum der Stadt Zürich von der Videoüberwachung betroffen ist. Die Beratung und Vermittlung würde nur auf Anfrage hin erfolgen und stets auf der freiwilligen Mitwirkung der Betroffenen basieren. Der Vorschlag des Stadtrats wurde der Geschäftsprüfungskommission als vorberatende Kommission zur weiteren Behandlung überwiesen.

Übersicht über weitere hängige politische Vorstösse zur Videoüberwachung

Im Berichtsjahr sind zum Thema Videoüberwachung zwei Motionen eingereicht worden:

Die Motion GR Nr. 2019/327 verlangt die Gleichstellung der Videoüberwachung mit und ohne Aufzeichnung und damit verbunden eine Anpassung der Datenschutzverordnung. Der Stadtrat lehnte die Entgegennahme dieser Motion ab und beantragte die Umwandlung in ein Postulat. Dabei wies der Stadtrat unter Verweis auf den Tätigkeitsbericht 2018 der Datenschutzstelle darauf hin, dass die Bestimmungen im Bereich Videoüberwachung nicht nur partiell bzw. Stück für Stück, sondern umfassend geprüft und angepasst werden sollten.

Die Motion GR Nr. 2019/57 verlangt die Einführung einer Bewilligungspflicht für die Überwachung des öffentlichen Raums durch private Videokameras. Der Stadtrat lehnte auch die Entgegennahme dieser Motion ab und beantragte auch hier die Umwandlung in ein Postulat. Er ist der Ansicht, dass ein öffentliches Interesse an der Regelung der Videoüberwachung des öffentlichen Grundes durch Private besteht. Allerdings ist die Rechtslage hinsichtlich der Zuständigkeiten unklar. Deshalb erachtet der Stadtrat es als zielführend, mit einem unabhängigen Rechtsgutachten abklären zu lassen, ob und gegebenenfalls in welcher Weise eine Bewilligungspflicht eingeführt werden könnte.

Bereits 2018 wurde dem Stadtrat ein Postulat eingereicht, welches die Kennzeichnung sämtlicher mobiler und standortgebundener Videoüberwachungskameras fordert. Anfang Januar 2020 wurde dieses Postulat nun zur Prüfung an den Stadtrat überwiesen.

FOKUS ENTWICKLUNG DES DATENSCHUTZRECHTS

Das Datenschutzrecht ist seit langem keine bloss nationale oder kantonale Angelegenheit mehr. Nebst der technologischen Entwicklung beeinflusst insbesondere das europäische Datenschutzrecht die schweizerische Gesetzgebung.

Datenschutzrecht in Europa

Das europäische Datenschutzrecht basiert im Wesentlichen auf drei Erlassen:

– Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europaratskonvention 108): Sie gilt international als datenschutzrechtlicher Minimalstandard und wurde 2018 aktualisiert. Für die Schweiz ist diese Konvention verbindlich.

– Datenschutz-Grundverordnung der Europäischen Union (DSGVO): Sie ist ein Rechtserlass der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Sie ist für alle EU-Mitgliedstaaten und EWR-Staaten verbindlich. Unter gewissen Umständen ist das Datenschutzrecht der Europäischen Union auch ausserhalb ihres Hoheitsgebietes anwendbar, beispielsweise für international tätige Unternehmen in der Schweiz. Für die städtische Verwaltung kann die DSGVO höchstens in (bisher noch nicht eingetretenen) Ausnahmefällen zur Anwendung kommen.

– EU-Richtlinie über den Datenschutz im Bereich der Strafverfolgung und des Strafvollzugs (Richtlinie Polizei und Justiz): Die Schweiz ist Mitglied des Schengen-Assoziierungsabkommens. Die Richtlinie ist deshalb auch für die Schweiz verbindlich.

Datenschutzrecht in der Schweiz

Das Bundesgesetz über den Datenschutz (DSG) regelt die Datenbearbeitung durch Bundesorgane sowie Privatpersonen und private Unternehmen. Das DSG gilt für kantonale und kommunale Verwaltungen grundsätzlich nicht.

Laufende Anpassungen: Um die EU-Richtlinie Polizei und Justiz zu erfüllen, hat der Bund ein Schengen-Datenschutzgesetz erlassen. Dieses ist am 1. März 2019 in Kraft getreten. Die Anpassung des DSG an die revidierte Europaratskonvention und die europäische DSGVO ist noch im Gange.

Datenschutzrecht im Kanton Zürich

Jeder Kanton hat ein eigenes Datenschutzgesetz, das für die Datenbearbeitung der kantonalen Verwaltung sowie der Gemeindeverwaltungen gilt. Für den Kanton Zürich und seine Gemeinden ist es das Gesetz über die Information und den Datenschutz (IDG).

Laufende Anpassungen: Um die EU-Richtlinie Polizei und Justiz zu erfüllen, hat der Regierungsrat im Sommer 2018 dem Kantonsrat eine Vorlage zur Revision des IDG unterbreitet. Der Kantonsrat hat diese im November 2019 einstimmig verabschiedet. Diese Revision des IDG tritt am 1. Juni 2020 in Kraft. Bereits eine weitere Revision hat der Regierungsrat mit Beschluss vom 4. März 2020 in Auftrag gegeben.

Datenschutzrecht in der Stadt Zürich

Ergänzend zum IDG hat der Gemeinderat der Stadt Zürich die städtische Datenschutzverordnung (DSV) erlassen. Sie regelt spezifische Datenschutz-Themen der Stadtverwaltung wie das Einwohnerregister oder die Videoüberwachung.

Aktuelle Revisionen des kantonalen Informations- und Datenschutzgesetzes

IDG-Revision zum Ersten …

Im Mai 2016 ist die EU-Richtlinie über den Datenschutz im Bereich der Strafverfolgung und des Strafvollzugs in Kraft getreten. Diese Richtlinie gehört zum Schengen-Recht, weshalb Bund und Kantone gemäss den Schengen-Assoziierungsabkommen verpflichtet sind, ihre Gesetze entsprechend anzupassen. Der Regierungsrat des Kantons Zürich überwies im Juli 2018 eine Vorlage zur Revision des kantonalen Informations- und Datenschutzgesetzes (IDG) an den Kantonsrat, welche sich auf den zwingenden Anpassungsbedarf gemäss EU-Richtlinie beschränkte. Der Kantonsrat verabschiedete die Vorlage ohne wesentliche Anpassungen im November 2019. In Kraft treten wird das revidierte IDG am 1. Juni 2020.

Neu ins IDG eingeführt wird eine Meldepflicht bei Datenschutzverletzungen. Verwaltungsstellen, die für eine Datenbearbeitung verantwortlich sind, müssen unbefugte Bearbeitungen oder den Verlust von Personendaten bei der Datenschutzstelle melden. Zu melden sind jedoch nur Vorfälle, die die Grundrechte betroffener Personen gefährden. Bagatellfälle ohne weitere Grundrechtsrelevanz sind damit von der Meldepflicht ausgenommen. Die Verwaltungsstellen haben auch die betroffenen Personen zu informieren, wenn die Datenschutzstelle es verlangt oder «wenn die Umstände es erfordern». Welche Umstände eine Meldung an die Betroffenen erforderlich machen, wird sich erst noch zeigen müssen, denn diese werden weder im Gesetz noch in den Erläuterungen des Regierungsrates näher umschrieben. Die Information an Betroffene kann aber auf alle Fälle ganz oder teil-

weise eingeschränkt werden, wenn überwiegende öffentliche oder private Interessen dagegensprechen. Eine Meldepflicht bei Datenschutzverletzungen kannte das Schweizerische Recht noch nicht. Auf Bundesebene wurde eine solche erstmals 2019 mit dem neuen Schengen-Datenschutzgesetz eingeführt.

Die Verwaltungseinheiten müssen bei einer beabsichtigten Bearbeitung von Personendaten mit einer sogenannten Datenschutz-Folgeabschätzung deren Risiken für die Grundrechte der betroffenen Personen bewerten. Diese Datenschutz-Folgeabschätzung soll eine allgemeine Beschreibung der geplanten Datenbearbeitungen, eine Bewertung der damit verbundenen Risiken sowie eine Darstellung der Massnahmen enthalten. Gemäss Weisung des Regierungsrats zur Revision IDG werde mit der Verpflichtung zur Durchführung einer Datenschutz-Folgeabschätzung grundsätzlich nichts Neues verlangt. In Bezug auf die Stadtverwaltung kann die Datenschutzstelle diese Einschätzung teilen. Die mit der Datenschutz-Folgeabschätzung verlangten Beschreibungen, Bewertungen und Darstellungen gehören bereits heute zum Inhalt und Prüfgegenstand des städtischen ISDS-Prozesses (vgl. Einleitungstext Seite 8).

Die Verwaltung soll die diversen datenschutzrechtlichen Vorgaben und Verpflichtungen nicht nur korrekt anwenden und umsetzen, sie soll die Einhaltung der Datenschutzbestimmungen auch nachweisen. Hierfür wird neu der Begriff der Organisationsvorschriften ins IDG eingeführt. Der Regierungsrat nennt in seiner Weisung zur Revision des IDG nebst Organisationsvorschriften auch Informationssicherheitsrichtlinien oder Zugriffskonzepte, die diesen Zweck der Nachweisbarkeit erfüllen sollen. Ähnlich wie vorstehend zur Datenschutz-Folgeabschätzung erwähnt, werden sich für die Stadtverwaltung auch hinsichtlich Einhaltung der Datenschutzbestimmungen keine grundlegend neuen Anforderungen ergeben.

Bereits unter geltendem Recht hat die oder der Datenschutzbeauftragte die Möglichkeit, gegen festgestellte Verletzungen von Datenschutzbestimmungen vorzugehen. Die geltenden Regelungen und Kompetenzen entsprechen jedoch nicht den Anforderungen der EU-Richtlinie. Neu wird die Datenschutzstelle bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form von Verfügungen treffen können, die von der betroffenen Dienstabteilung beim Verwaltungsgericht angefochten werden können. Die Verfügungskompetenz der Datenschutzstelle beschränkt sich jedoch auf erhebliche Verletzungen von Datenschutzbestimmungen.

Mit der Revision des IDG werden genetische und biometrische Daten ausdrücklich in die Kategorie der besonderen Personendaten aufgenommen. Ebenfalls in diese Kategorie fällt neu das Profiling, also die automatisierte Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen. Will die Verwaltung Daten bearbeiten, die als besondere Personendaten qualifiziert werden, bedarf sie einer genügend bestimmten Regelung in einem formellen Gesetz.

IDG-Revision zum Zweiten ...

Der Regierungsrat Zürich hat bereits im Juli 2018, als er die vorstehend erwähnte IDG-Revision initiierte, mitgeteilt, dass weiterer Anpassungsbedarf in einem gesonderten Revisionsprojekt geprüft werde. Dieses Projekt hat er nun formell mit Beschluss vom 4. März 2020 in Auftrag gegeben. Revisionsbedarf beim IDG hat sich in den vergangenen Jahren aus unterschiedlichen Gründen ergeben: Die Evaluation des IDG in den Jahren 2013 – 2017 zeigte diverse Optimierungsmöglichkeiten auf. Verschiedene politische Vorstösse im Kantonsrat betreffen das Datenschutzrecht und das Öffentlichkeitsprinzip. Die Digitalisierung der Verwaltung bringt mit sich, dass Behördendaten vermehrt als strategische Ressourcen zu verstehen und zu nutzen sind. Und schliesslich zeigt sich Anpassungsbedarf im täglichen Umgang mit dem IDG in den Verwaltungen von Kanton und Gemeinden.

Unter der Leitung des Generalsekretariats der Direktion Justiz und Inneres wird nun ein Projektteam einen entsprechenden Vernehmlassungsentwurf erarbeiten. Der Datenschutzbeauftragte der Stadt Zürich ist Mitglied dieses Projektteams.

Feststellungen und Beurteilungen

Kontrolle OMEGA-Online

Verwaltungsinterner Online-Zugriff auf das städtische Einwohnerregister

In der Stadt Zürich besteht seit über 15 Jahren für zahlreiche Dienstabteilungen die Möglichkeit, Daten aus dem Einwohnerregister online abzufragen. In den letzten Jahren wurde das bisherige System ALPHA im Rahmen eines mehrjährigen Projekts durch das System OMEGA abgelöst. Unabhängig davon, ob die Dienstabteilungen bereits über einen Online-Zugang zu Daten des Einwohnerregisters verfügten, mussten sie mit dem Systemwechsel auf OMEGA den Zugang beim Bevölkerungsamt neu beantragen.

Die städtische Datenschutzverordnung verlangt, dass jede Dienstabteilung, die Daten aus dem Einwohnerregister beziehen will, mit einem schriftlichen Gesuch beim Bevölkerungsamt die benötigten Personendaten je mit Beschreibung des Verwendungszwecks beantragen und die Notwendigkeit für einen Online-Zugriff begründen muss. Das Bevölkerungsamt, das für die Führung des Einwohnerregisters verantwortlich ist, prüft, ob die beantragten Zugriffe mit Blick auf die gesetzlichen Aufgaben der jeweiligen Dienstabteilungen plausibel und erforderlich sind, und erteilt oder verweigert die Zugriffsberechtigung. Für den technischen Betrieb des Systems OMEGA ist die Dienstabteilung Organisation und Informatik (OIZ) zuständig. Sie ist es dann auch, die die jeweiligen Zugriffe entsprechend der Instruktion des Bevölkerungsamtes freischaltet.

Prüfung und Feststellungen der Datenschutzstelle

Rund 30 Dienstabteilungen der Stadt Zürich sowie einige wenige Verwaltungsstellen des Kantons Zürich wurden vom Bevölkerungsamt bisher berechtigt, über das System OMEGA Daten aus dem Einwohnerregister online abzufragen. Die Datenschutzstelle hat im Berichtsjahr kontrolliert, ob bei den erteilten Berechtigungen die materiellen und formellen Vorgaben eingehalten wurden. Die Datenschutzstelle hat hierfür vom Bevölkerungsamt alle Gesuche, Entscheide und schriftlichen Instruktionen herausverlangt und anlässlich mehrerer Besprechungen diverse Fragen geklärt. Sie konnte dabei Folgendes feststellen:

– Für alle auf das System OMEGA berechtigten Verwaltungsstellen liegen die notwendigen Gesuche und Entscheide im Sinne der Datenschutzverordnung vor.

  Das Bevölkerungsamt hat das Antragsverfahren standardisiert und hierfür ein ausgeklügeltes, mehrseitiges Formular ausgearbeitet, welches durch die Dienstabteilungen auszufüllen ist. Im Formular werden alle Angaben verlangt, wie sie die städtische Datenschutzverordnung vorsieht.

– Das Bevölkerungsamt hat sichergestellt, dass die berechtigten Verwaltungsstellen nur die für die Erfüllung ihrer gesetzlichen Aufgaben notwendigen Daten abrufen können.

  Das System OMEGA fasst die einzelnen Daten des Einwohnerregisters zu zehn Datenblöcken zusammen. Bei den Gesuchen ist anzugeben, welche Datenblöcke benötigt werden. Dabei müssen die Dienstabteilungen Angaben zum Verwendungszweck machen und begründen, weshalb sie hierfür einen Online-Zugriff benöti-

gen. Auch müssen die Dienstabteilungen Angaben zur Anzahl der zugriffsberechtigten Mitarbeitenden machen. Die Zusammenfassung der Personendaten aus dem Einwohnerregister zu einzelnen Datenblöcken erfolgt thematisch geordnet und die Aufteilung in diese zehn unterschiedlichen Daten- bzw. Rechteblöcke erlaubt eine genügende Differenzierung im Sinne des Verhältnismässigkeitsgrundsatzes. Aus den Entscheiden des Bevölkerungsamtes geht nachvollziehbar hervor, auf welche Datenblöcke Zugriff gewährt und auf welche Zugriff abgelehnt wurde.

– Das Bevölkerungsamt hat bei allen Gesuchen die Notwendigkeit eines Online-Zugriffs überprüft.

  Für die Überprüfung der Notwendigkeit eines Online-Zugriffs im Einzelfall hat das Bevölkerungsamt die folgenden Kriterien angewandt: Einerseits das Mengengerüst an Datenanfragen und andererseits die zeitliche Dringlichkeit, in welcher Auskünfte über Daten aus dem Einwohnerregister vorliegen müssen. Diese Kriterien waren nach Ansicht der Datenschutzstelle verständlich und das Bevölkerungsamt hat gegenüber der Datenschutzstelle glaubhaft dargelegt, dass bei den einzelnen Gesuchen die Erfüllung der Kriterien, insbesondere auf Grundlage entsprechender Kennzahlen, kontrolliert wurden.

– Die Instruktionen des Bevölkerungsamtes an die OIZ erfüllten die datenschutzrechtlichen Anforderung nicht.

  Die OIZ ist für die technische Freischaltung der Zugriffsberechtigungen zuständig. Diese Freischaltung hat nach verbindlichen, nachvollziehbaren und formellen Instruktionen des Bevölkerungsamtes zu erfolgen. Diese wiesen bisher Defizite auf. Das Bevölkerungsamt hat die OIZ zwar darüber informiert, ob und mit welchen

Berechtigungen die Online-Zugriffe zu gewähren sind, formelle Instruktionsentscheide jedoch fehlten. Die Datenschutzstelle hat dieses Defizit beanstandet und verlangte eine entsprechende Nachbesserung.

Zusätzlich zu den kontrollierten Anforderungen müssen bei OMEGA weitere Voraussetzungen erfüllt werden – insbesondere im Bereich der Informationssicherheit. Geprüft wurden diese Anforderungen bereits während der Projektabwicklung im Rahmen des ISDS-Prozesses (vgl. Einleitungstext Seite 8). Wie bei der Inbetriebnahme solcher Systeme in der Stadtverwaltung üblich, wurden einzelne sicherheitstechnische Massnahmen zudem im Rahmen eines Audits durch eine externe Firma kontrolliert.

Nachbesserung durch das Bevölkerungsamt

Das Bevölkerungsamt hat die beanstandeten Instruktionsentscheide umgehend angepasst und hierfür das Formular, welches für das Antragsverfahren und die Entscheide des Bevölkerungsamtes eingesetzt wird, entsprechend ergänzt. Das Formular beinhaltet nun klare und schlüssige Instruktionsentscheide, welche der beantragten Datenblöcke durch die OIZ freizuschalten sind. Neu verlangt das Bevölkerungsamt, dass die Freischaltungen schriftlich in Form von Vollzugsmeldung durch die OIZ bestätigt werden. Auch diese Vollzugsmeldungen erfolgen auf dem Standardformular. Damit werden sämtliche verfahrensnotwendigen Informationen in einem einzigen Formular erfasst, was die Nachvollziehbarkeit des gesamten Verfahrens – vom Antrag bis zur Bestätigung der Freischaltung – gewährleistet.

Automatisierte Fahrzeugfahndung und Verkehrsüberwachung

Der Strassenverkehr wird in der Schweiz zunehmend mit Hilfe technischer Überwachungsmassnahmen kontrolliert. Vielerorts im Einsatz war die sogenannte Automatisierte Fahrzeugfahndung und Verkehrsüberwachung (AFV). Mit diesem System werden die Nummernschilder von Fahrzeugen erfasst und in Sekundenbruchteilen mit polizeilichen Datenbanken abgeglichen. Befindet sich ein Nummernschild in einer dieser Datenbanken, wird eine Meldung («hit») ausgelöst, die es der Polizei ermöglicht, das Fahrzeug entsprechend zu kontrollieren. Die Nummernschilder der Fahrzeuge, welche in keiner der verknüpften Datenbanken enthalten sind, werden zwar auch erfasst, die erhobenen Informationen werden jedoch unverzüglich und ohne weitere Bearbeitung automatisch gelöscht («no-hit»).

Die Stadtpolizei setzte bis anhin AFV mit zwei mobilen Geräten und einer stationären Anlage ein. Verknüpft waren dabei das Schweizerische Polizeifahndungssystem RIPOL, welches gestohlene Fahrzeuge und solche ohne Versicherungsschutz registriert, die kantonale Datenbank über die Fahrzeugausweisentzüge im Kanton Zürich sowie die städtische Radschuhliste, die ausländische Fahrzeuge enthält, für die offene Bussen bestehen und deren Halter- und Lenkerschaft nicht ermittelt werden kann. Im Tätigkeitsbericht 2015 hat die Datenschutzstelle ausführlich über den Einsatz und die datenschutzrechtliche Beurteilung der AFV in der Stadt Zürich informiert.

Im Herbst 2019 stellte die Stadtpolizei Zürich ihre AFV ein. Grund dafür ist ein Bundesgerichtsurteil von Oktober 2019, in welchem die AFV der Kantonspolizei Thurgau untersucht und wegen nicht ausreichender Rechtsgrundlage als nicht zulässig beurteilt wurde. Da die

vom Bundesgericht definierten gesetzgeberische Anforderungen an die AFV von allgemeiner Bedeutung und auch im Kanton Zürich nicht erfüllt sind, wird die Stadtpolizei Zürich die AFV erst wieder einsetzen, wenn die hierfür erforderlichen Rechtsgrundlagen vorhanden sind.

Gemäss Bundesgericht stellt die AFV einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Verkehrsteilnehmenden dar. Mit derartigen automatisierten Systemen werde eine massenhafte und praktisch unbegrenzte Erhebung von Daten ermöglicht, was eine erhebliche Erhöhung der polizeilichen Überwachungs- und Fahndungsintensität zur Folge habe. Durch die Verknüpfung mit anderen polizeilichen Datenbanken ermögliche die AFV die serielle und simultane Verarbeitung grosser und komplexer Datensätze innert Sekundenbruchteilen, was insofern über die herkömmliche verkehrstechnische Informationsbeschaffung und die Fahndungssysteme der bisherigen sicherheitspolizeilichen Gefahrenabwehr hinausgehe. Mit der Überwachung durch AFV bestehe die Gefahr, dass Persönlichkeits- oder Bewegungsprofile gebildet würden oder Betroffene zu Unrecht in Verdacht gerieten. Letzteres zeige die erhebliche Fehlerquote im beurteilten System des Kantons Thurgau auf.

Aufgrund der Schwere des Grundrechtseingriffs verlangt das Bundesgericht angemessene und wirkungsvolle rechtliche Schutzvorkehrungen, um Missbräuchen und Willkür vorzubeugen. Die Rechtsgrundlagen, auf die sich die Polizei für den Einsatz solcher Systeme abstützen wolle, müsse insbesondere den Verwendungszweck, den Umfang der Erhebung sowie die Aufbewahrung und Löschung der Daten klar und bestimmt regeln. Für die Strassenverkehrsteilnehmenden müsse es vorhersehbar sein, welche Informationen gesammelt, aufbewahrt und mit anderen Datenbanken verknüpft werden. Im Gesetz müsse die Reichweite des Datenabgleichs sachbezogen

eingegrenzt und die Pflicht zur unverzüglichen und spurlosen Löschung im Nichttrefferfall («no-hit») festgeschrieben werden.

Trotz dem auf den ersten Blick klaren Verdikt des Bundesgerichts werden aber noch einige Fragen zu klären sein. So fragt sich, ob die erforderlichen Rechtsgrundlagen tatsächlich (nur) in den kantonalen Polizeigesetzen geschaffen werden müssen, zumal das Schweizerische Polizeifahndungssystem RIPOL und auch weitere verknüpfte Datenbanken vor allem nationale Datenbanken sind. Eine vergleichbare Frage wird sich auch hinsichtlich der städtischen Radschuhliste stellen. Da es sich hierbei um eine Datenbank der Stadt Zürich handelt, wird die Frage zu klären sein, ob die Legitimation für deren Einbindung in die AFV der Stadtpolizei mit der noch zu erarbeitenden kantonalen Rechtsgrundlage geschaffen wird oder ob die Stadt Zürich hierfür eigenständig eine gesetzliche Grundlage erlassen muss.

Zuteilung der Schülerinnen und Schüler

Im Herbst des Berichtsjahres berichteten verschiedene Medien, dass das städtische Schulamt eine neue Applikation für die Zuteilung der Stadtzürcher Schülerinnen und Schüler in die einzelnen Schulhäuser und Klassen im Rahmen der Klassenbildung auf den Beginn einer Schulstufe hin einsetze. Im Rahmen dieser Berichterstattung wurde kritisiert, dass diese neue Applikation fragwürdige Informationen über die Schülerinnen und Schüler enthalte und ohne Wissen und Einwilligung der Erziehungsberechtigten genutzt werde. Zudem sei nicht erkennbar, wer welche Informationen eintrage und eine Löschung der Daten finde während der gesamten Schullaufbahn der Kinder nicht statt. Diese Berichterstattung veranlasste die Datenschutzstelle, die kritisierte Applikation einer datenschutzrechtlichen Prüfung zu unterziehen.

Die Schülerinnen- und Schülerzuteilung nach Klassen und Schulhäusern

Alle Schülerinnen und Schüler der Stadt Zürich werden während ihrer obligatorischen Schullaufbahn dreimal in Schulhäuser und Klassen zugeteilt. Diese Zuteilungen finden jeweils vor einem Stufenübertritt, also jeweils im zweiten Semester des zweiten Kindergartenjahres sowie der dritten und der sechsten Primarklasse, statt. Ziel der Zuteilung ist eine ausgewogene Klassenzusammensetzung. Die Kriterien, die dies sicherstellen sollen, werden in der kantonalen Volksschulgesetzgebung sowie in einem Reglement der Schulpflege der Stadt Zürich beschrieben: Massgebend für die Zuteilung sind die soziale und sprachliche Herkunft, die Leistungsfähigkeit sowie die Verteilung

der Geschlechter. Zu berücksichtigen ist ausserdem die Länge und Gefährlichkeit des Schulwegs. Zusätzlich zu diesen Kriterien schreiben die erwähnten gesetzlichen Grundlagen vor, wer für die Zuteilung zuständig ist. So nehmen die Schulpflegen bzw. in der Stadt Zürich die Präsidentinnen oder Präsidenten der Kreisschulbehörden die Zuteilung der Schülerinnen und Schüler in die Schulhäuser vor, während die Schulleitungen diejenige in die Klassen innerhalb einer Schule übernehmen.

Um diese gesetzlichen Vorgaben umzusetzen, entwickelte das Schulamt das sogenannte SKS-Tool. SKS steht für «Standardisierte Kriterien Schülerzuteilung».

Feststellungen und Beurteilungen der Datenschutzstelle

Die Zuteilung der Schülerinnen und Schüler stellt wie erwähnt eine Pflicht aus der Volksschulgesetzgebung dar. Kreisschulbehörden, Schulleitungen und Klassenlehrpersonen sind verpflichtet und legitimiert, die zum Zweck der Zuteilung notwendigen Schülerinnen- und Schülerdaten zu bearbeiten. Eine Einwilligung der Erziehungsberechtigten zur Bearbeitung dieser Informationen oder zur Nutzung des SKS-Tools ist damit nicht erforderlich. Ob und in welcher Weise es angezeigt ist, die Erziehungsberechtigten über die Zuteilung und die damit verbundene Datenbearbeitung zu informieren, ist weniger eine datenschutzrechtliche als vielmehr eine Frage der Zusammenarbeit bzw. Kommunikation zwischen Schule und Eltern. Laut Schulamt sind die für die Schülerinnen- und Schülerzuteilung relevanten Informationen den Erziehungsberechtigten bereits vor deren Eintrag ins SKS-Tool bekannt. Dies deshalb, weil sie sich auf die bisherigen schulischen Leistungen der Schülerinnen und Schüler abstützen, weil individuelle Fördermassnahmen stets das Einverständnis der

Erziehungsberechtigten voraussetzen und weil sonstige für die Zuteilung relevante Punkte bei Elterngesprächen zu thematisieren sind.

Im SKS-Tool tragen die Klassenlehrpersonen je nach Übertrittsstufe Noten und/oder Niveaus der Hauptfächer ein, bewerten die Sach-, Sozial- und Selbstkompetenzen der Schülerinnen und Schüler und vermerken deren Inanspruchnahme individueller Fördermassnahmen wie beispielsweise integrative Förderung, Deutsch als Zweitsprache oder Logopädie. Damit werden ausschliesslich Angaben zu Schülerinnen und Schülern erfasst, die der vorstehend erwähnten gesetzlich umschriebenen Zuteilung dienen.

Die erwähnten Angaben, die durch die Klassenlehrpersonen in das SKS-Tool eingetragen werden, sind durch die Schulbehörden vordefiniert. Für die Einträge stehen somit standardisierte Eingabefelder zur Verfügung. Weil laut Schulamt jedoch nicht für alle zuteilungsrelevanten Kriterien standardisierte und vordefinierte Eingaben möglich sind, beinhaltet das SKS-Tool zusätzlich ein Freitextfeld. Darin können die Klassenlehrpersonen ergänzende Bemerkungen erfassen, sofern dies für die Klassenzuteilung erforderlich ist. Es war vor allem dieses Freitextfeld, das Anlass zu eingangs erwähnter Kritik gab, da darin in Einzelfällen fragwürdige Informationen festgehalten wurden, deren Relevanz zur Zuteilung nicht ohne Weiteres ersichtlich war. Damit künftig besser sichergestellt werden kann, dass nur Angaben oder Informationen im Freitextfeld erfasst werden, die für die Zuteilung der Schülerinnen und Schüler relevant sind, wurde ein diesbezüglicher Hinweis ins SKS-Tool eingefügt. Zusätzlich dazu weisen die Schulbehörden die Klassenlehrpersonen mit Anleitungen zum SKS-Tool an, im Freitextfeld nur Angaben einzutragen, die für die Zuteilung relevant sind.

Die Datenschutzstelle konnte feststellen, dass sich die Zugriffe auf das SKS-Tool an den gesetzlichen Zuständigkeiten der Schülerinnen- und Schülerzuteilung orientieren. Den weitreichendsten Zugriff benötigen die Präsidentinnen und Präsidenten der Kreisschulbehörden bzw. die beauftragten Behördenmitglieder, da sie die Schülerinnen und Schüler teilweise schulkreisübergreifend zuteilen müssen. Die Zuteilung der Schülerinnen und Schüler in die Klassen einer Schule ist durch die Schulleitung vorzunehmen. Ihr Zugriff erstreckt sich daher auf die Informationen sämtlicher Schülerinnen und Schüler ihrer Schule. Die Beurteilung der Schülerinnen und Schüler erfolgt wie erwähnt durch die Klassenlehrpersonen. Dazu reicht ihnen ein Zugriff auf die Informationen der eigenen Klasse. Wie bei städtischen Informatikprojekten üblich, werden auch beim SKS-Tool sämtliche Zugriffe, Einträge und Änderungen automatisch protokolliert, damit die erforderliche Nachvollziehbarkeit gewährleistet werden kann.

Nach der verbindlichen Zuteilung der Schülerinnen und Schüler auf die Schulhäuser und in die Klassen hat das SKS-Tool seinen Zweck erfüllt. Ein Zugriff auf die darin eingetragenen Daten ist nicht mehr notwendig. Daher werden sämtliche Zugriffsberechtigungen nach Abschluss der Zuteilungen entzogen. Zu welchem Zeitpunkt nach Abschluss der jährlichen Zuteilung die Daten im SKS-Tool zu löschen sind, ist noch Gegenstand von Abklärungen. Dies deshalb, weil das Schulamt diese Daten allenfalls für Auswertungen oder Forschungsvorhaben benötigen wird. Sofern die Daten im SKS-Tool auch für solche – auf alle Fälle nicht schülerinnen- und schülerbezogene – Zwecke zur Verfügung stehen sollen, sind sie den üblichen datenschutzrechtlichen Anforderungen entsprechend so rasch wie möglich zu anonymisieren.

Das SKS-Tool wurde der Datenschutzstelle vor Inbetriebnahme nicht via städtischem ISDS-Prozess (vgl. Einleitungstext Seite 8) zur Prüfung angemeldet. Das Schulamt überprüfte und optimierte zwischenzeitlich seine diesbezüglichen internen Prozesse. In Bezug auf das SKS-Tool verlangte die Datenschutzstelle vom Schulamt ein Konzept, welches sämtliche relevanten Modalitäten der Datenbearbeitung nachvollziehbar und verbindlich regelt.

Interview

«Privatsphäre – geschützt, geteilt, verkauft»

Im Zürcher Stadthaus war von September 2019 bis Februar 2020 die Ausstellung «Privatsphäre – geschützt, geteilt, verkauft» zu sehen. Sie thematisierte eindrücklich, wie wichtig und gleichzeitig nur schwer fassbar die Privatsphäre ist. Die Ausstellung zeigte, wie Privatheit abhängig von Moralvorstellungen und Sicherheitsbedürfnissen und somit dem steten Wandel unterworfen ist und wie widersprüchlich unser Verhältnis zu ihr sein kann. Beleuchtet wurden unterschiedlichste Themenbereiche aus dem Alltag: Etwa der Umgang mit Körper und Intimität, die Diskussion um öffentliche und private Räume, die Bedeutung von Exklusivität und Geheimnissen oder der Handel mit digitalen Daten. Die Ausstellung stiess auf reges Publikumsinteresse. Zahlreiche Schulklassen haben sie besucht und alle grösseren Zeitungen haben über sie berichtet.

Co-Kuratorin dieser Ausstellung war Dr. Sarah Genner. Sie ist Medienwissenschaftlerin, Digitalexpertin und Dozentin. Ihr Spezialgebiet sind die Auswirkungen digitaler Medien auf Mensch, Gesellschaft und Arbeitswelt.

Was veranlasste die Kulturabteilung der Stadt Zürich, gemeinsam mit dem Collegium Helveticum eine Ausstellung zum Thema Privatsphäre durchzuführen? Gab es bestimmte Gründe hierfür?

Stadt Zürich Kultur macht im Stadthaus Zürich jedes Jahr eine gesellschaftspolitische Ausstellung. Wie verschiedene Städte schreibt sich auch Zürich auf die Fahnen, eine «Smart City» zu sein. Eine sinnvolle Nutzung von Daten und Digitaltechnologien hat für die Bevölkerung zahlreiche Vorteile, bringt aber auch Fragestellungen rund um Privat-

sphäre und Datenschutz mit sich. Insofern kam der thematische Impuls neben der Digitalisierung und populären Sozialen Medien auch aus der Stadtentwicklung. Der Kulturwissenschaftler Christian Ritter und ich wurden seitens der Stadt angefragt, ob wir die Ausstellung gemeinsam kuratieren möchten. Wir arbeiten beide seit vielen Jahren wissenschaftlich zu Themen rund um digitale Medien und Gesellschaft und suchen den Austausch mit einer interessierten Öffentlichkeit. Dass am Collegium Helveticum gegenwärtig eine Forschungsperiode zum Thema «Digital Societies» läuft, in deren Rahmen auch zu Fragen der Privatsphäre gearbeitet wird, war für uns eine zusätzliche Möglichkeit, die Ausstellung nahe an der aktuellen Forschung zu entwickeln.

Der Begriff der Privatsphäre scheint auf den ersten Blick klar und verständlich zu sein. Wie sieht es aus, wenn genauer hingeschaut wird?

Für Christian Ritter und mich war es sehr befriedigend, dass wir das Thema Privatsphäre so breit und auch historisch angehen konnten. Es liegt auf der Hand: Anlass, warum wieder häufiger über Privatsphäre debattiert wird, ist die zunehmende Digitalisierung. Der Blick in die Vergangenheit zeigt jedoch, wie sich in den Diskussionen um Privatsphäre der gesellschaftliche Wandel spiegelt – aber auch das politische Klima und die Moralvorstellungen der jeweiligen Zeit. Es ist beim genaueren Hinsehen nicht eindeutig, dass wir heute über weniger Privatsphäre verfügen als früher, obwohl das heute ein Allgemeinplatz ist. Was wir im Alltag unter «Privatsphäre» verstehen, ist individuell und abhängig von Interessen. Nicht immer sind sich Bürgerinnen und Bürger, Firmen und Behörden einig, wo Privatsphäre beginnt und wo sie enden soll. Denn es bestehen zahlreiche Widersprüche: Wir sagen zwar, Privatsphäre sei uns wichtig, aber wir verhalten uns – gerade online – oft nicht entsprechend. Und wir wollen sehen und gesehen werden. Ausserdem wollen wir gleichzeitig

Sicherheit und Freiheit. Für Kriminelle fordern wir maximale Überwachung. Aber was, wenn massenhaft Unschuldige überwacht werden, um wenige Kriminelle und potenzielle Terroristen im Auge zu behalten? Uns hat die Herausforderung Spass gemacht, die Ausstellung wissenschaftlich fundiert und zugleich für ein breites Publikum zugänglich zu machen und die genannten Widersprüche darzustellen.

In der Ausstellung konnten die Besucherinnen und Besucher ein Infoblatt zur «Digitalen Selbstverteidigung» mitnehmen. Darin wurde aufgefordert, den Datenschutz selbst in die Hand zu nehmen, und es wurden Tipps im Umgang mit Passwörtern, Smartphone, E-Mail, Internet und Social Media erteilt. Wie viel Selbstverteidigung braucht die Privatsphäre wirklich? Und gäbe es nicht andere Möglichkeiten, die für jede und jeden von uns mit weniger Mühe und Aufwand verbunden wären?

Selbstversändlich wäre es wünschenswert, wenn die Privatsphäre keine Angelegenheit der «Selbstverteidigung» wäre. Dafür setzen sich zum Glück auch Datenschutzbehörden unermüdlich ein, die jedoch angesichts der enormen Zunahme an Aufgaben kaum nachkommen. Zudem ist es rechtlich schwierig, international tätige Firmen in die Schranken zu weisen. Einerseits sammeln viele dieser Firmen halbwegs legal Daten, weil User die Nutzungsbedingungen mit einem Klick ungelesen bestätigen, andererseits ist Recht national organisiert, was einer globalen Infrastruktuktur wie dem Internet kaum gerecht werden kann. Bis politisch griffige Gesetze für digitalen Datenschutz und deren Durchsetzung gesichert sind, bleibt fast nur eine gewisse «Verteidigung» auf individueller Ebene.

Digitale Selbstverteidigung oder mindestens digitale Kompetenz benötigen wir nicht mehr nur wegen den grossen Tech-Giganten aus dem Silicon Valley. Auch Schweizer Medienhäuser interessieren sich

zunehmend für unsere persönlichen Daten. So haben diverse von ihnen beispielsweise damit begonnen, ihre Informationen im Netz nur noch gegen persönliche Registrierung zur Verfügung zu stellen. Was halten Sie von dieser Entwicklung? Welchen Einfluss wird die Personalisierung auf die Medien und unseren Medienkonsum haben?

Dass Schweizer Medienhäuser Leserinnen und Leser online registrieren, ist angesichts der Medienkrise auch verständlich. Viele haben über lange Jahre online aufwändige Recherchen gratis zur Verfügung gestellt und müssen nun verzweifelt ihre Bezahlschranken hochfahren. Persönliche Registrierung ist ein Mittel dafür. Andererseits sammeln sie sehr wahrscheinlich gleichzeitig auch auf unlautere Weise Daten, nach welchen die Werbewirtschaft dürstet, die dort möglichst passgenaue Inserate schalten soll. Personalisierte Werbung ist das Geschäft der Zukunft. Einer Personalisierung der Inhalte stehe ich zwiespältig gegenüber: Einerseits kann es befriedigend sein, Medieninhalte vorgeschlagen zu bekommen, für die man sich interessiert. Andererseits besteht die Gefahr, dass uns in einer Demokratie die Basis für gesamtgesellschaftliche Debatten fehlt, wenn alles personalisiert wird. Ich sehe diese Tendenz im Moment allerdings kaum.

Die Corona-Krise der letzten Wochen und Monate forderte uns alle sehr. Eine Herausforderung dabei war die zunehmende Einschränkung des öffentlichen Lebens und der Zwang zum Rückzug ins Private. Welche Rolle spielte dabei die Digitalisierung? Erleichterte sie uns diese Herausforderung?

Zugespitzt kann man sagen: Das Coronavirus, Home Office und Home Schooling entpuppen sich gerade als grösste Digitalisierungsoffensive des 21. Jahrhunderts. Dank digitaler Technologien können wir informiert bleiben, kommunizieren, arbeiten, Schule weiterführen und uns unterhalten lassen, während wir aufgefordert sind, uns in

unsere Privaträume zurückzuziehen. Gleichzeitig entsteht viel Öffentlichkeit über soziale Medien und Einblicke in Privaträume durch Videokonferenzen, Berichte darüber, was Menschen zuhause machen, wie sie Kinder und Arbeit zuhause unter einen Hut bringen. Digitaltechnologien ermöglichen vieles, aber gleichzeitig übt ihr Vorhandensein auch einen starken Druck aus, von zuhause aus zu arbeiten und online zu lernen, weil es eben möglich ist. Das kann für einige weniger digital Geübte auch eine Krise in der Krise sein.

Wird diese Krise die Einstellung unserer Gesellschaft zur Digitalisierung nachhaltig verändern? Wird es mit der Digitalisierung jetzt erst recht und schneller vorwärts gehen?

Prognosen sind oft schwierig. Persönlich vermute ich, dass diese Krise und gewissermassen schlagartig erzwungene Digitalisierung eine polarisierende Wirkung haben wird. Wer ohnehin technisch begeistert ist, wird sich jetzt noch mehr bestätigt fühlen. Wer bereits kritisch unterwegs war, findet vermutlich noch zusätzlich: Jetzt sitzen wir alle noch mehr hinter diesen Bildschirmen und liefern Datensammlern noch mehr Daten.

Privatsphäre ist eine relativ junge Errungenschaft unserer Gesellschaft. Sie entstand mit dem Aufkommen des Bürgertums. Mit zunehmender Technologisierung und Digitalisierung sehen viele das Ende der Privatsphäre sich abzeichnen. Werden Privatsphäre und Privatheit als blosse Episode in die Geschichte der Menschheit eingehen?

Persönlich sehe ich keineswegs ein «Ende der Privatsphäre» im digitalen Zeitalter. Früher hatten viele durch eine höhere Sozialkontrolle auf dem Land weniger Privatsphäre als nach der Urbanisierung. In der Stadt geniesst man durch die Grösse eine höhere Privatsphäre,

obwohl man näher zusammenwohnt. 45 % der Haushalte in Zürich sind inzwischen Einpersonenhaushalte: Die räumliche Privatsphäre hat so gesehen eher zugenommen. Interessant sind Befragungen, die zeigen, dass sich Menschen online gar nicht so sehr vor datensammelnden Firmen oder Geheimdiensten verstecken wollen, sondern vor ihrem Arbeitgeber, ihren Lebenspartnern, vor gewissen Freundinnen oder Bekannten aus der Vergangenheit. Insofern halte ich folgende Frage für interessant: Privatsphäre für wen und vor wem?

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%)

Gestaltung:
Stadt Zürich, Züriblau

Stadt Zürich
Datenschutzstelle
Beckenhofstrasse 59
8006 Zürich
Tel. 044 412 16 00
datenschutz@zuerich.ch
www.stadt-zuerich.ch/datenschutz