



20
18

«Ah, du arbeitest im Bereich Datenschutz. Interessant. Und hochaktuell! Ihr habt sicher viel zu tun. Aber ... was genau macht ihr eigentlich? Wie muss ich mir eure Arbeit vorstellen?»

Geschätzte Leserinnen und Leser

So oder ähnlich sind die Reaktionen, wenn Mitarbeitende einer Datenschutzstelle sagen, wo sie arbeiten. Das grosse Interesse, das dem Thema Datenschutz und unserer Tätigkeit entgegengebracht wird, freut uns sehr. Damit noch besser verstanden werden kann, was wir tun, haben wir unseren Tätigkeitsbericht angepasst: In einem ersten Teil ([Grundlagen](#)) stellen wir die Datenschutzstelle der Stadt Zürich und unsere Tätigkeiten vor und erklären kurz und bündig, um was es im Datenschutzrecht geht. Anschliessend berichten wir über thematische [Schwerpunkte](#) aus dem Jahr 2018. Hierfür fokussieren wir uns auf sieben Themen innerhalb des Datenschutzrechts und veranschaulichen diese mit Beispielen aus dem Berichtsjahr. In einem dritten Teil äussern wir uns zu wichtigen [Feststellungen und Beurteilungen](#). Abschliessen möchten wir unseren Bericht wie in den vergangenen Jahren auch mit einer Sicht von aussen. Im diesjährigen [Interview](#) erfahren Sie von zwei Mitarbeitenden städtischer Rechtsdienste, die auch die Funktion als Datenschutz-BeraterIn ausüben, wie sie den Datenschutz in der Stadtverwaltung Zürich wahrnehmen und einschätzen.

Wir hoffen, Ihnen mit diesem Bericht nicht nur unsere Tätigkeiten, Aufgaben und Themen näher bringen, sondern auch eine interessante Lektüre bieten zu können. Für Ihr Interesse danken wir Ihnen sehr.

Datenschutzstelle der Stadt Zürich
Marcel Studer, Datenschutzbeauftragter

Inhaltsverzeichnis

Grundlagen	6
Die Datenschutzstelle der Stadt Zürich kurz vorgestellt	7
Das Datenschutzrecht kurz erklärt	13
Schwerpunkte	16
FOKUS	
Die digitale Stadtverwaltung	17
Online-Beratung beim Laufbahnzentrum	19
Online-Formular für Stipendienanträge	21
Online-Subventionsantrag für Kita-Plätze	22
E-Vermietung	23
Parking-App (bargeldloses Parkieren)	26
FOKUS	
Auskunft über eigene Personendaten	29
Einsicht in die Bilder der Blitzkasten	31
FOKUS	
Forschung, Planung und Statistik	34
Qualitätsnachweis bei Notrufeinsätzen	36
FOKUS	
Informationsverwaltung	38
Papierakten bei Mitgliedern von Kommissionen oder Behörden	39

FOKUS	
Entwicklung des Datenschutzrechts	41
Anwendungsbereich der DSGVO	43
FOKUS	
Personalbereich	46
Mobiles Arbeiten	48
Digitales Personaldossier	51
FOKUS	
Videoüberwachung	54
Beratungen und Prüfungen im Bereich Videoüberwachung	56
Feststellungen und Beurteilungen	58
Videoüberwachung	59
Städtisches Zugangsportaal «Mein Konto»	66
Interview	70
Die städtischen Beraterinnen und Berater für Datenschutz	71

Grundlagen

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

Wer sind wir?

Die Datenschutzstelle der Stadt Zürich besteht aus dem Datenschutzbeauftragten, 3 juristischen Mitarbeitenden und einer Sekretariatsmitarbeiterin. Insgesamt teilen wir uns 3 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 9 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.

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

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

- **Projekte der Stadtverwaltung prüfen und beraten**

Heutzutage gibt es kaum noch Daten, die nicht mittels moderner Informations- und Kommunikationstechnik (ICT) bearbeitet werden. In der Stadtverwaltung Zürich müssen sämtliche Projekte, die ICT betreffen, den sogenannten Informationssicherheits- und Datenschutz-Prozess (ISDS-Prozess) durchlaufen. Auf diesem Wege werden jährlich durchschnittlich 40–60 Projekte aus der gesamten Stadtverwaltung der Datenschutzstelle zur Prüfung vorgelegt. 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.

- **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 ist 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

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

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.

– [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.

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

- **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 und Bedürfnisse umgesetzt werden. Um einen möglichst sachgerechten Umgang mit Daten erreichen zu können, bedarf es organisationsübergreifender und interdisziplinärer Zusammenarbeit. Insbesondere ...

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

- ... 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. Diese 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. Im Interview am Schluss des vorliegenden Tätigkeitsberichts stellen eine Beraterin und ein Berater ihre Funktion und Tätigkeit näher vor (Seite 70).

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

- ... mit Datenschutzbeauftragten der Kantone und des Bundes

Die Datenschutzbeauftragten der Kantone und des Bundes arbeiten über ihren schweizerischen Verband 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.

Das Datenschutzrecht kurz erklärt

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). 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. Für weitere Ausführungen zu den diversen Datenschutzgesetzen vgl. [Seiten 41](#).

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 Bürger 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:

Das Datenschutzrecht kurz erklärt

- *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 ihre Einwohnerinnen und Einwohner bearbeiten darf, ergibt sich aus den gesetzlichen Grundlagen der jeweiligen Verwaltungsbe-
reiche: also beispielsweise aus der Polizei-, Sozialhilfe-, Gesundheits- oder Schulgesetzgebung.
- *Zweckbindung*: Die Verwaltung darf Personendaten nur zu dem Zweck bearbeiten, zu dem 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 Löschrufen 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 über sensible Datenbearbeitungen adressatengerecht informieren und allenfalls Organisationsvorschriften erlassen muss.

Schwerpunkte

FOKUS

Die digitale Stadtverwaltung

Vom e-Banking bis zum Kleiderkauf im Webshop – wir alle nutzen privat immer mehr Online-Angebote. Auch von der öffentlichen Verwaltung wird zunehmend erwartet, dass ihre Dienste online verfügbar sind. Mit dem Strategieschwerpunkt «Digitale Stadt» setzt sich der Stadtrat zum Ziel, die digitalen Angebote für die Bevölkerung laufend auszubauen.

Mit «[Mein Konto](#)» vereinfacht die Stadt Zürich sukzessive den Zugang der Bevölkerung zu den Dienstleistungen der Verwaltung. Immer mehr Online-Angebote der Stadtverwaltung sind über dieses zentrale Zugangsportal (www.stadt-zuerich.ch/meinkonto) erreichbar.

Zu diesen Angeboten gehören insbesondere Anmeldungen, Gesuche, Bestellungen oder Terminvereinbarungen. Für solche Prozesse müssen immer auch persönliche Daten der Bürgerinnen und Bürger erhoben und bearbeitet werden. Die Transformation ins digitale Zeitalter ist ein idealer Zeitpunkt, bisherige Geschäftsprozesse und damit verbundene Datenbearbeitungen kritisch zu hinterfragen. Zu prüfen ist dabei stets auch die [Verhältnismässigkeit](#), also die Frage, ob nur diejenigen Daten bearbeitet werden, welche für die Erfüllung der öffentlichen Aufgabe effektiv notwendig sind.

Persönliche Daten müssen geschützt werden, insbesondere vor unberechtigtem Zugriff. Der [Zugang](#) zu den meisten städtischen Online-Diensten ist nur möglich, wenn vorgängig ein persönliches Benutzerkonto erstellt wurde. Bei jeder Anmeldung überprüft das System, ob Benutzername und Passwort mit den Informationen im

FOKUS

Die digitale Stadtverwaltung

persönlichen Benutzerkonto übereinstimmen. Bei diesem technischen Prüfvorgang spricht man von **Authentifizierung**. Für den Zugriff auf sensible Personendaten wird zusätzlich die Eingabe eines temporären Codes verlangt, welcher beispielsweise auf das Handy geschickt wird. In solchen Fällen spricht man von 2-Faktor-Authentifizierung.

Mit der Authentifizierung einer Person ist noch nicht sichergestellt, dass diese tatsächlich diejenige ist, welche sie vorgibt zu sein. Bei vielen Verwaltungsprozessen wird deshalb ein Identitätsnachweis verlangt. Aktuell besteht noch keine Möglichkeit, eine solche **Identifizierung** ausschliesslich digital durchzuführen. Entsprechende Bestrebungen für die Schaffung einer sogenannten digitalen Identität sind auf Bundesebene im Gange. Bis es soweit ist, müssen die Verwaltungsstellen die Identität auf der Grundlage von amtlichen Dokumenten oder mit Hilfe bestehender Datenbanken, wie beispielsweise dem Einwohnerregister, individuell überprüfen.

Zum Fokus *Die digitale Stadtverwaltung* stellen wir folgende Beispiele aus dem Berichtsjahr vor:

- Online-Beratung beim Laufbahnzentrum
- Online-Formular für Stipendienanträge
- Online-Subventionsantrag für Kita-Plätze
- E-Vermietung
- Parking-App (bargeldloses Parkieren)

Im Kapitel **Feststellungen und Beurteilungen** weisen wir auf den Regelungsbedarf hin, der nach Ansicht der Datenschutzstelle im Zusammenhang mit dem Zugangsportale «Mein Konto» besteht.

Online-Beratung beim Laufbahnzentrum

Ob bei der Ärztin, beim Psychologen oder beim Berufs-, Studien- und Laufbahnberater: Persönliche Gespräche setzen Vertrauensräume voraus, in welchen sich die Beteiligten frei äussern können. In der analogen Welt finden solche Gespräche im Sprechzimmer von Angesicht zu Angesicht statt. Vermehrt werden solche Vertrauensräume in den digitalen Bereich verlagert. Bereits sind verschiedene Online-Anwendungen auf dem Markt, welche das herkömmliche Sprechzimmer quasi digital simulieren.

Das Laufbahnzentrum der Stadt Zürich zieht in Betracht, künftig Beratungsdienstleistungen auch online anzubieten und hierzu eine bereits etablierte Internetplattform für die Online-Beratung einzusetzen. Über die Plattform können Termine vereinbart, Gespräche mit Videotelefonie geführt oder Chatnachrichten ausgetauscht werden. Auch können Inhalte auf einem elektronischen Flipchart festgehalten werden. Chatverlauf und Flipchart werden gespeichert und können bei Folgeberatungen wieder hervorgeholt werden. Diese Plattform wird durch eine externe Firma betrieben, weshalb die Datenschutzstelle sie zusammen mit der Fachstelle Informationssicherheit genauer unter die Lupe genommen hat. Die Prüfung der Plattform ergab, dass die Sicherheitsanforderungen grundsätzlich erfüllt sind. Defizite konnten allerdings festgestellt werden bezüglich des Zugriffs auf die gespeicherten Chatverläufe und Inhalte des Flipcharts. Da es sich dabei um sensible Inhalte handeln kann, muss der Online-Zugriff auf diese Inhalte durch eine 2-Faktor-Authentifizierung geschützt werden. Eine solche Funktion fehlt bisher.

FOKUS

Die digitale Stadtverwaltung

Ob beim Laufbahnzentrum die Internetplattform für die Online-Beratung künftig zum Einsatz kommt, wird sich erst noch zeigen. Das Laufbahnzentrum testet vorerst im Rahmen eines Pilotversuchs, ob diese einerseits beim Zielpublikum auf Anklang stösst und andererseits die Bedürfnisse des Laufbahnzentrums erfüllt. Die Datenschutzstelle erachtete es für vertretbar, dass der Pilotversuch noch ohne 2-Faktor-Authentifizierung erfolgt. Dies unter der Voraussetzung, dass der Pilotversuch nur mit wenigen ausgewählten Testpersonen durchgeführt wird und das Laufbahnzentrum diese vorgängig über die Risiken im Zusammenhang mit der Speicherung der Chatverläufe und des Flipcharts informiert.

Unabhängig davon, ob die Nutzung der Plattform nur im Pilotbetrieb oder allenfalls definitiv erfolgt: Die Nutzung einer Online-Beratung erfolgt freiwillig. Das Laufbahnzentrum will seine Beratungsleistungen auch weiterhin Personen zur Verfügung stellen, welche das herkömmliche «Sprechzimmer» bevorzugen.

Online-Formular für Stipendienanträge

Wer bei der Stadt Zürich Stipendien für eine Ausbildung beantragt, muss viele persönliche Daten offenlegen. Dies verlangt das städtische Stipendienrecht, welches regelt, wer Stipendien erhält. Zuständig für die Prüfung der Stipendienanträge ist das Laufbahnzentrum der Stadt Zürich. Dieses hat die Online-Angebote für seine Kundschaft erweitert. Unter anderem werden Stipendienanträge in Zukunft auf der Grundlage eines elektronischen Formulars online bearbeitet.

Das im Datenschutzrecht geltende Verhältnismässigkeitsprinzip verlangt, dass nur diejenigen Personendaten erhoben und bearbeitet werden, welche für die Erfüllung einer gesetzlichen Aufgabe notwendig sind. Die Datenschutzstelle konnte im Rahmen einer Vorabkontrolle feststellen, dass sich das Laufbahnzentrum bei der Ausarbeitung des Online-Formulars gezielt mit den Anforderungen an die Verhältnismässigkeit auseinandergesetzt und nachvollziehbar dargelegt hat, auf welche Daten es für den Stipendienentscheid angewiesen ist. Auch konnte die Datenschutzstelle feststellen, dass die Sicherheit dieses Formulars technisch gewährleistet ist. Das Online-Formular ist in das städtische Zugangsportal «Mein Konto» eingebunden. Eine 2-Faktor-Authentifizierung schützt das Formular vor unberechtigten Zugriffen. Der Identitätsnachweis erfolgt anhand von amtlichen Dokumenten, welche dem Gesuch beizufügen sind, sowie mittels Online-Abfragen aus dem Einwohnerregister.

Online-Subventionsantrag für Kita-Plätze

Seit Herbst 2018 haben Eltern in der Stadt Zürich die Möglichkeit, ihren Antrag auf einen subventionierten Kita-Platz online über das städtische Portal «Mein Konto» zu stellen. Das Sozialdepartement bearbeitet diese Anträge, prüft den konkreten Bedarf von Eltern an einem subventionierten Betreuungsplatz und legt deren Anspruch individuell fest. Um festzustellen, ob Eltern einen Anspruch auf einen subventionierten Kita-Platz haben, benötigt das Sozialdepartement umfangreiche Angaben der Eltern. Es klärt nicht nur ab, ob Eltern ein subventionierter Kita-Platz zugeteilt werden kann, sondern bemisst auch den Umfang, sprich die genaue Anzahl Tage, an denen ein solcher Platz besucht werden darf. Dabei spielt es mitunter eine Rolle, wie hoch der Beschäftigungsgrad der Eltern ist, ob sie auf Arbeitssuche sind oder eine Ausbildung absolvieren.

Die Datenschutzstelle qualifizierte die Angaben, welche Eltern im Zusammenhang mit einem Subventionsantrag machen, teilweise als sensibel, so beispielsweise die Angabe der RAV-Vermittlungsfähigkeit von Eltern. Dies gilt aber auch für die Tatsache des Stellens eines Subventionsantrags an sich: Im Zusammenhang mit dem Antrag werden viele Daten erhoben und bearbeitet, welche einzeln nicht unbedingt als sensibel zu qualifizieren sind. In ihrer Summe können sie jedoch derart viel über eine einzelne Person aussagen, dass von einem sogenannten «Persönlichkeitsprofil» auszugehen ist, welches ebenfalls als sensibel qualifiziert werden muss. Aus diesen Gründen verlangte die Datenschutzstelle für den Zugang zum Subventionsantrag über «Mein Konto» eine sogenannte 2-Faktor-Authentifizierung.

E-Vermietung

In der Stadt Zürich sind per 1. Januar 2019 die neue Vermietungsverordnung sowie das dazugehörige Mietreglement in Kraft getreten. Diese Rechtsgrundlagen schreiben vor, nach welchen Grundsätzen und unter welchen Bedingungen die Stadt Zürich ihre Wohnungen, die zur Kostenmiete vermietet werden, zu vermieten hat. Im Wesentlichen sind dies:

- Vielseitige Zusammensetzung der Mieterschaft;
- Wohnsitzpflicht in der Stadt Zürich;
- Angemessenes Verhältnis zwischen Wohnungsgrösse und Zahl der Bewohnerinnen und Bewohner;
- Angemessenes Verhältnis zwischen Mietzins und den wirtschaftlichen Verhältnissen der Bewohnerinnen und Bewohner.

Diese Grundsätze und Bedingungen sind auch aus datenschutzrechtlicher Sicht massgebend, wirken sie sich doch unmittelbar auf die Erhebung und weitere Bearbeitung von Personendaten aus. Sie legitimieren und verpflichten die Stadt Zürich, die erforderlichen Angaben und Informationen der Mietinteressentinnen und -interessenten zu bearbeiten, setzen ihr gleichzeitig aber auch Schranken, die hinsichtlich Datenbearbeitung nicht überschritten werden dürfen.

FOKUS

Die digitale Stadtverwaltung

Damit die Vermietungsgrundsätze mit modernen und effizienten Mitteln umgesetzt werden können, hat die Dienstabteilung *Liegenschaften Stadt Zürich* den Service «E-Vermietung» eingeführt. Über das städtische Zugangsportale «Mein Konto» können sich Interessentinnen und Interessenten für die Wohnungsbesichtigung anmelden. Aus den Interessentinnen und Interessenten, die die Vermietungskriterien erfüllen, wählt ein Zufallsgenerator eine bestimmte Anzahl aus, die zur Besichtigung eingeladen werden. Diejenigen, die an der Wohnungsbesichtigung teilnehmen konnten, erhalten wiederum über «Mein Konto» die Möglichkeit, sich auf die Wohnung zu bewerben.

Im Rahmen einer Vorabkontrolle überprüfte die Datenschutzstelle insbesondere die Verhältnismässigkeit der Erhebung und weiteren Verwendung der persönlichen Angaben von Mietinteressentinnen und -interessenten. Dabei konnte festgestellt werden, dass Liegenschaften Stadt Zürich genau prüfte und nachvollziehbar darlegte, welche Daten zu welchem Zeitpunkt zur Überprüfung der gesetzlichen Bedingungen benötigt werden. So wird insbesondere klar getrennt zwischen Anmeldung zur Wohnungsbesichtigung und Bewerbung auf eine Mietwohnung. Wer eine Wohnung besichtigen möchte, muss neben den Personalien die Anzahl Personen angeben, die die Wohnung beziehen möchten. Bereits mit diesen Angaben kann Liegenschaften Stadt Zürich überprüfen, ob die Interessentinnen und Interessenten die gesetzlichen Kriterien an eine Vermietung dem Grundsatz nach erfüllen und damit überhaupt zu einer Wohnungsbesichtigung eingeladen werden können. Wer sich anschliessend für eine Wohnung bewerben will, muss Liegenschaften Stadt Zürich umfassende Informationen zu persönlichen, familiären und finanziellen Verhältnissen einreichen, damit die Bedingungen der neuen städtischen Vermietungsverordnung überprüft werden können.

FOKUS

Die digitale Stadtverwaltung

Auch eine Frage der Verhältnismässigkeit ist die Aufbewahrungsdauer beziehungsweise die Löschung von Personendaten. In der E-Vermietungsapplikation werden die Daten der ausgeschiedenen Interessentinnen und Interessenten umgehend nach der Auswahl durch den Zufallsgenerator gelöscht. Die Daten der zur Besichtigung eingeladenen Interessentinnen und Interessenten sowie ihrer anschliessenden Bewerbung bleiben während eines Jahres gespeichert. Zudem wird jede relevante Bewertung, Priorisierung und Auswahl dokumentiert und ebenfalls für ein Jahr gespeichert. Damit wird die in der Vermietungsverordnung verlangte Nachvollziehbarkeit und Dokumentation des Vermietungsverfahrens sichergestellt. Ein Zugriff auf die gespeicherten Daten ist daher auch nur für Aufsichts- oder Revisionszwecke zulässig. Die Prüfung der Datenschutzstelle hat gezeigt, dass Liegenschaften Stadt Zürich den Grundsatz der Verhältnismässigkeit einhält und korrekt mit den persönlichen Angaben der Mietinteressentinnen und -interessenten umgeht.

Parking-App (bargeldloses Parkieren)

Seit April 2019 können in der Stadt Zürich die Gebühren für öffentliche Parkplätze per App bargeldlos bezahlt werden. Dazu können die Automobilistinnen und Automobilisten unter drei privaten App-Anbietern auswählen. Die App-Anbieter speisen die Informationen zu den Parkvorgängen ihrer Kundinnen und Kunden in eine eigens hierfür errichtete zentrale Datenbank der Stadt Zürich ein. Schwerpunkt der Beratung und Prüfung durch die Datenschutzstelle war denn auch diese neue städtische Datenbank und die damit verbundene Datenbearbeitung. In Anbetracht dessen, dass es sich im Zusammenhang mit der Bezahlung von Parkgebühren per App um eine Datenbearbeitung im polizeilichen Kontext handelt, viele Personen davon betroffen sein können und mehrere städtische Verwaltungsstellen involviert sind, verlangte die Datenschutzstelle, dass die wichtigsten Modalitäten verbindlich, klar und nachvollziehbar geregelt werden. Im Wesentlichen betraf dies folgende Punkte:

- **Zweck der zentralen Datenbank**

Aus datenschutzrechtlicher Sicht ist stets der Zweck einer Datenbearbeitung der massgebende Ausgangspunkt. Es muss klar sein, wozu Daten bearbeitet werden. Die Personendaten in der zentralen Datenbank dienen der Kontrolle der Parkvorgänge. Zusätzlich dazu wird anhand der Daten in der zentralen Datenbank die Belegung der Parkzonen ausgewertet. Dies geschieht ausschliesslich mit anonymisierten Daten, weshalb diese Auswertung datenschutzrechtlich nicht weiter von Relevanz ist.

FOKUS

Die digitale Stadtverwaltung

- **Definition der erforderlichen Daten**

In die zentrale Datenbank eingespielen werden dürfen nur diejenigen Daten, die für die Kontrolle von Parkvorgängen erforderlich sind. Es sind dies im Wesentlichen das Kontrollschild, der Beginn und das Ende des Parkvorgangs sowie die Nummer und Bezeichnung der Parkzone.

- **Zugriffsregelung**

Wer auf welche Daten Zugriff haben darf, muss in einem Berechtigungs- und Zugriffskonzept festgelegt werden. Dieses hat sich am Zweck der zentralen Datenbank, somit also an der Kontrolle der Parkvorgänge, auszurichten.

- **Speicherung und Löschung der Daten**

Für die Kontrolle der Parkvorgänge werden die Daten in der zentralen Datenbank für die Dauer von 24 Stunden benötigt. Anschließend werden die Daten anonymisiert, so dass keine Personendaten mehr vorhanden und nur noch Auswertungen ohne Rückschlussmöglichkeit auf Automobilistinnen und Automobilisten möglich sind.

- **Regelung von Zuständigkeiten und Verantwortung**

Wenn mehrere Verwaltungseinheiten einen gemeinsamen Informationsbestand bearbeiten, müssen sie ihre Verantwortlichkeiten regeln. Im Zusammenhang mit der zentralen Datenbank und der Kontrolle von Parkvorgängen stehen sowohl der Dienstabteilung Verkehr als auch der Stadtpolizei Aufgaben und Kompetenzen zu. Die jeweiligen Zuständigkeiten und Verantwortungen sind deshalb entsprechend zu regeln.

FOKUS

Die digitale Stadtverwaltung

Das Sicherheitsdepartement der Stadt Zürich ist der Forderung der Datenschutzstelle nachgekommen und hat für den Betrieb der zentralen Datenbank verbindliche Organisationsvorschriften erlassen, die die erwähnten Modalitäten regeln.

FOKUS

Auskunft über eigene Personendaten

Datenschutz bedeutet nicht nur, dass Personendaten vor unrechtmässiger Bearbeitung oder Kenntnisnahme geschützt werden. Das Datenschutzrecht gibt den Bürgerinnen und Bürgern auch das Recht, Auskunft über die eigenen Personendaten zu erhalten, die bei der Stadtverwaltung vorhanden sind.

Der datenschutzrechtliche Anspruch auf Auskunft bezieht sich nicht auf alle Informationen, sondern nur auf **eigene Personendaten**, also nur auf diejenigen Daten, die die gesuchstellende Person selber betreffen. Darüber hinaus ist Auskunft auch über die Rechtsgrundlage, die die Stadtverwaltung zur Bearbeitung der fraglichen Personendaten ermächtigt, den Bearbeitungszweck sowie die regelmässigen Adressaten der Daten zu erteilen. Die Auskunft kann ganz oder teilweise eingeschränkt werden, wenn ein Gesetz dies vorsieht oder wenn überwiegende öffentliche oder private Interessen dies verlangen. **Einschränkungen** dürfen aber immer nur soweit erfolgen, wie sie sowohl inhaltlich als auch zeitlich notwendig sind.

Wer eine Auskunft über eigene Personendaten erhalten will, stellt ein **schriftliches Gesuch** an diejenige Verwaltungsstelle, die die gewünschten Personendaten bearbeitet. Die gesuchstellende Person muss ihr Gesuch nicht begründen. Sie muss sich aber **identifizieren**, am besten mit einer Kopie eines Personalausweises. Die Auskunft ist in der Regel innert 30 Tagen mittels **Zustellung von Kopien** zu erteilen. Für die Auskunft über eigene Personendaten werden keine Gebühren erhoben.

FOKUS

Auskunft über eigene Personendaten

Zum Fokus *Auskunft über eigene Personendaten* stellen wir aus dem Berichtsjahr das Beispiel der Blitzkasten im Strassenverkehr vor.

Einsicht in die Bilder der Blitzkasten

Wer in der Stadt Zürich zu schnell oder bei Rot über die Kreuzung fährt und dabei geblitzt wird, bekommt von der Stadtpolizei eine Busse. Was die Autofahrerinnen oder Autofahrer aber nicht bekommen, sind die Bilder der Blitzkasten, auch nicht auf Anfrage hin. Eine Privatperson wandte sich an die Datenschutzstelle mit der Frage, ob die Stadtpolizei Zürich damit nicht das Recht auf Einsicht in die eigenen Personendaten verletze.

Fehlende Regelung im Ordnungsbussenverfahren

Das Prinzip der Busse im Strassenverkehr kennen wohl einige Automobilistinnen und Automobilisten: Sich ärgern, Busse bezahlen und fertig. Das sogenannte Ordnungsbussenverfahren vereinfacht den Umgang mit geringfügigen Delikten für alle Beteiligten. Das Verfahren ist rasch und einfach. Die Sache ist erledigt, wenn die Busse innert 30 Tagen bezahlt wird. Wird die Busse jedoch innert dieser Frist nicht bezahlt, überweist die Polizei das Verfahren an die Strafuntersuchungsbehörden. Nicht geregelt im Ordnungsbussenverfahren ist jedoch, ob die Polizei innerhalb der 30-tägigen Zahlfrist einer Automobilistin oder einem Automobilisten Einsicht in die Bilder der Blitzkasten geben muss. Aus dieser fehlenden gesetzlichen Regelung leitete die Stadtpolizei bisher ab, eine Einsicht in die Bilder müsse nicht gewährt werden.

FOKUS

Auskunft über eigene Personendaten

Das Recht auf Einsicht als elementarer Bestandteil der Rechtsordnung

Die Rechte auf Einsicht in Verfahrensakten und in eigene Personendaten sind elementare Bestandteile unserer Rechtsordnung und in der Verfassung garantiert. Eine Einschränkung dieser Rechte wie beispielsweise die grundsätzliche Verweigerung von Bildern der Blitzkasten ist nur zulässig, wenn ein Gesetz dies ausdrücklich so vorsieht. Aus dem Umstand, dass sich das Ordnungsbussenverfahren zur Akteneinsicht oder zur Einsicht in eigene Personendaten nicht äussert, darf folglich nicht abgeleitet werden, dass solche elementaren Ansprüche unserer Rechtsordnung in diesem Verfahren nicht bestehen.

Und der damit verbundene Aufwand?

Die Stadtpolizei begründet ihre bisherige Praxis auch damit, dass die Einsicht in die Bilder der Blitzkasten der Raschheit und Effizienz des Ordnungsbussenverfahrens widerspreche und einer kostengünstigen Erledigung von Bagatelldelikten entgegenstehe. Eine Einsicht in die Bilder verursacht unbestrittenermassen Aufwand: Die Identität der anfragenden Person muss geprüft werden und die Einsicht in die Bilder muss aufgrund der kurzen gesetzlichen Zahlungsfrist rasch erfolgen können. Dennoch vertritt die Datenschutzstelle die Ansicht, dass ein grundsätzlicher Ausschluss des Rechts, Einsicht in die Bilder der Blitzkasten zu nehmen, nicht zu rechtfertigen ist.

FOKUS

Auskunft über eigene Personendaten

Der Aufwand, der bei Gesuchen um Einsicht in die Bilder der Blitzkasten anfallen wird, darf nach Ansicht der Datenschutzstelle zudem nicht isoliert nur mit Blick auf die Stadtpolizei beurteilt werden. Werden Bussen dank Einsicht in die Bilder bereits bei der Stadtpolizei akzeptiert und bezahlt, können damit aufwendigere und kostenpflichtige Verfahren bei der Strafuntersuchungsbehörde vermieden werden.

Praxisänderung

Die Datenschutzstelle ist gestützt auf diese Erwägungen zum Schluss gekommen, dass den gebüssten Automobilistinnen und Automobilisten auch im Ordnungsbussenverfahren ein Recht auf Einsicht in die Bilder der Blitzkasten zusteht. Die Stadtpolizei teilte der Datenschutzstelle mit, dass sie ihre Praxis ändern werde.

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».

Die Stadtverwaltung ist grundsätzlich berechtigt, ihre Daten auch zu Forschungs-, Planungs- oder Statistikzwecken zu nutzen. Sie muss dabei sicherstellen, dass Personendaten sobald als 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 diese 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 durch strenge Zugriffsregeln geschützt

FOKUS

Forschung, Planung und Statistik

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.

Zum Fokus *Forschung, Planung, Statistik* stellen wir aus dem Berichtsjahr das Beispiel der Qualitätsnachweise bei Notrufeinsätzen bei Schutz & Rettung Stadt Zürich vor.

Qualitätsnachweis bei Notrufeinsätzen

Bei Notrufeinsätzen müssen die Abläufe sitzen und es darf nichts dem Zufall überlassen werden. Schnelles und korrektes Handeln der Mitarbeitenden kann darüber entscheiden, ob Personen überleben. Permanente Analysen der Notrufeinsätze sollen Hinweise auf Defizite geben und dazu beitragen, die Qualität der Notrufeinsätze laufend zu verbessern. Wie es in der Forschung, der Planung oder der Statistik üblich ist, braucht es für solche Analysen grundsätzlich keine Personendaten. In rechtlicher Hinsicht handelt es sich bei Qualitätsnachweisen deshalb um Datenbearbeitungen zu sogenannten nicht personenbezogenen Zwecken.

Datenlager für Qualitätsanalysen

Die städtische Dienstabteilung Schutz & Rettung ist als Betreiberin der Notrufzentrale für die Leitung der Einsätze und damit auch für die Qualitätssicherung verantwortlich. Um die Qualität von Notrufeinsätzen besser analysieren zu können, hat sie eigens hierfür ein Datenlager (neudeutsch: Data Warehouse) aufgebaut. Als Quelle für das Datenlager dient das operative System der Notrufzentrale, somit eine Datenbasis mit zum Teil sensiblen Personendaten. Die für die Analysen benötigten Daten werden jeweils über Nacht in das Datenlager kopiert. Bei der Übernahme der Daten aus dem System der Notrufzentrale in das Datenlager wird soweit wie möglich auf identifizierende Angaben wie Namen, Vornamen oder Geburtsdatum verzichtet. Nicht verzichtet werden kann allerdings auf Angaben zu den jeweiligen Einsatzorten. Diese Angaben sind notwendig für Auswertungen zu den sogenannten Hilfsfristen. Darunter ist die Zeit zu verstehen, innerhalb welcher die Rettungskräfte am Einsatzort sein müssen. In der Stadt Zürich gilt eine Hilfsfrist von 10 Minuten.

FOKUS

Forschung, Planung und Statistik

Schutz & Rettung hat sich zum Ziel gesetzt, diese Vorgabe in 90 % der Einsätze zu erreichen. Der Einsatzort kann unter Umständen Rückschlüsse auf Personen ermöglichen, insbesondere wenn der Einsatzort sich an deren Wohnort befindet. Im Datenlager von Schutz & Rettung sind somit Informationen enthalten, die Personendaten darstellen und entsprechend geschützt werden müssen.

Massnahmen zum Schutz der Daten

Die Datenschutzstelle hat das Datenlager von Schutz & Rettung im Rahmen einer Vorabkontrolle geprüft. Dabei hat sie ein besonderes Augenmerk auf die Ausarbeitung eines verbindlichen Zugriffskonzepts gelegt. In diesem Konzept wird festgelegt, dass nur autorisierte Mitarbeitende von Schutz & Rettung, welche mit Aufgaben des Qualitätsmanagements betraut sind, Zugriff auf diese Daten haben. Der Datenschutzstelle war zudem wichtig, dass Schutz & Rettung dokumentiert, welche Auswertungen vorgenommen werden und wer hierfür zuständig ist. Die Anforderungen an die Informationssicherheit wurden auf der Grundlage eines Informationssicherheits- und Datenschutzkonzepts geprüft. Die Datenschutzstelle konnte sich hierbei – wie bei städtischen ICT-Projekten üblich – auf die technische Beurteilung der Fachstelle Informationssicherheit der Dienstabteilung OIZ abstützen.

FOKUS

Informationsverwaltung

Von der Verwaltung wird erwartet, dass sie mit ihren Akten und Informationen richtig umgeht. Die Verwaltung muss gewährleisten, dass geschäftsrelevante Informationen **vollständig** und richtig sind und berechtigten Personen bei Bedarf **zur Verfügung stehen**. Jede Datenbearbeitung muss zudem **erkennbar** sein und einer bestimmten Person **zugerechnet** werden können. Informationen müssen **vertraulich** behandelt und zur richtigen Zeit **archiviert oder gelöscht** werden.

Mit einer korrekten Informationsverwaltung soll erreicht werden, dass das Verwaltungshandeln **nachvollziehbar** ist und über dieses jederzeit **Rechenschaft** abgelegt werden kann. Zudem muss stets geklärt sein, welche Verwaltungsstelle für eine Informationsbearbeitung **verantwortlich** ist.

Die Stadtverwaltung hat im Jahr 2015 das sogenannte **Records Management** eingeführt. In mehreren Richtlinien, Leitfäden und Checklisten sind Grundsätze und Organisationsprinzipien für den richtigen Umgang mit Akten und Informationen festgehalten und umschrieben. Das Records Management ist für alle Organisationseinheiten der städtischen Verwaltung verbindlich.

Zum Fokus *Informationsverwaltung* stellen wir aus dem Berichtsjahr eine Anfrage zur Aktenaufbewahrung in privaten Räumlichkeiten von Mitgliedern bei Kommissionen oder Behörden vor.

Papierakten bei Mitgliedern von Kommissionen oder Behörden

Bei der Stadtverwaltung Zürich arbeiten nicht nur Mitarbeitende, welche hauptberuflich für die Stadt Zürich arbeiten und einen fixen Arbeitsplatz in einem Verwaltungsgebäude haben. Insbesondere bei Verwaltungsstellen wie Kommissionen oder Behörden arbeiten regelmässig auch Personen, die meist nur nebenberuflich öffentliche Aufgaben ausüben und hierfür über keinen Arbeitsplatz in der Verwaltung verfügen. Solche Miliz-Angestellte treffen sich lediglich zu Sitzungen oder Verhandlungen in Räumlichkeiten der Stadtverwaltung. Im Berichtsjahr erhielt die Datenschutzstelle die Anfrage, ob es solchen Miliz-Angestellten der Verwaltung gestattet sei, dienstliche Unterlagen bei sich zu Hause aufzubewahren.

Für die Beantwortung dieser Frage ist in erster Linie der Zweck der fraglichen Unterlagen massgebend: Wozu dienen diese und inwiefern lässt sich dieser Zweck mit der Aufbewahrung von Unterlagen bei Miliz-Angestellten zu Hause vereinbaren? In der Regel erhalten Miliz-Angestellte Papierakten als Arbeitsinstrument nach Hause zugestellt, um sich auf die Sitzungen oder Verhandlungen vorzubereiten. Wenn nach durchgeführter Sitzung oder Verhandlung die jeweiligen Geschäfte oder Dossiers abgeschlossen werden können, hat sich der Zweck der zugestellten Papierakten erfüllt. Beinhalten die Unterlagen Personendaten, ist eine weitere Aufbewahrung bei den Miliz-Angestellten bei sich zu Hause mit dem datenschutzrechtlichen Zweckbindungsprinzip nicht mehr zu vereinbaren. Dieses Prinzip verlangt, dass Personendaten nur zu dem Zweck bearbeitet werden, für welchen sie erhoben, beziehungsweise an die Mitglieder von Kommissionen oder Behörden zugestellt wurden.

Eine Möglichkeit, Unterlagen oder Akten bei Miliz-Angestellten allenfalls dennoch weiterhin aufzubewahren, wäre deren Anonymisierung. Um dies zu erreichen, müssten die Unterlagen derart bearbeitet werden, dass kein Rückschluss auf Personen mehr möglich ist, auch nicht aus dem Sachverhalt oder dem Kontext. Bei Geschäften oder Dossiers mit umfangreichen Angaben über Klientinnen oder Gesuchsteller wird eine Anonymisierung realistischlicherweise nicht möglich sein.

Die Datenschutzstelle hat bei der Beantwortung dieser Anfrage auch darauf aufmerksam gemacht, dass nicht nur die einzelnen Miliz-Angestellten für den richtigen Umgang mit dienstlichen Akten oder Unterlagen verantwortlich sind. Eine diesbezügliche Mit- oder sogar Hauptverantwortung obliegt (auch) der jeweiligen Kommission oder Behörde. Diese hat dafür zu sorgen, dass ihre Mitglieder wissen, wie sie mit Akten umzugehen haben. Sie hat sicherzustellen, dass ihre Akten nur so lange wie nötig und nur für deren bestimmungsgemässen Gebrauch bei den einzelnen Mitgliedern aufbewahrt und anschliessend korrekt vernichtet werden.

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:

1. *Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europaratskonvention 108)*
Die Europaratskonvention 108 gilt international als datenschutzrechtlicher Minimalstandard und wurde 2018 aktualisiert. Für die Schweiz ist diese Konvention verbindlich.
2. *Datenschutz-Grundverordnung der Europäischen Union (DSGVO)*
Die Datenschutz-Grundverordnung ist eine Verordnung 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.
3. *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.

FOKUS

Entwicklung des Datenschutzrechts

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 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. Das Geschäft ist pendent.

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.

Anwendungsbereich der DSGVO

Im Berichtsjahr trat die Datenschutzgrundverordnung (DSGVO) in der EU und dem EWR in Kraft und sorgte in der Schweiz nicht nur bei privaten Unternehmen, sondern auch in der Verwaltung der Stadt Zürich für grosse Verunsicherung. Viele Dienstabteilungen der Stadtverwaltung gelangten mit der Frage an die Datenschutzstelle, ob sie unter den Anwendungsbereich der DSGVO fallen.

Ob die DSGVO zur Anwendung kommt, bestimmt sich in Nicht-EU- oder Nicht-EWR-Staaten nach zwei besonderen Prinzipien: dem Niederlassungs- und dem Marktortprinzip.

Das Niederlassungsprinzip

Hat ein Datenbearbeiter – wie beispielsweise ein internationaler Versicherungskonzern – eine Niederlassung in einem Mitgliedsland der EU, muss er die Vorschriften der DSGVO einhalten. Für die Stadtverwaltung trifft dieses Kriterium kaum zu, da sie ihre Büros und Dienststellen in aller Regel in der Stadt Zürich und nicht auch als Niederlassung in einem Mitgliedsland der EU oder des EWR hat. Daher dürfte die DSGVO für die Stadtverwaltung gestützt auf das Niederlassungsprinzip kaum zur Anwendung kommen.

FOKUS

Entwicklung des Datenschutzrechts

Das Marktortprinzip

Fehlt es an einer Niederlassung in einem Mitgliedsland der EU, kann die DSGVO zur Anwendung kommen, wenn jemand Waren oder Dienstleistungen gezielt in Mitgliedsländern der EU anbietet. Ein solch gezieltes Angebot kann beispielsweise vorliegen, wenn ein Unternehmen besonders attraktive Lieferbedingungen bei einem Versand in ein Mitgliedsland der EU anbietet oder wenn es eine Kontaktadresse und Telefonnummer aus einem Mitgliedsland der EU veröffentlicht. Ob ein solches Angebot im Sinne des Marktortprinzips vorliegt, muss in jedem Fall einzeln beurteilt werden. Auch aufgrund des Marktortprinzips wird die DSGVO für die Stadtverwaltung kaum Anwendung finden, da sie – soweit der Datenschutzstelle bekannt – Waren oder Dienstleistungen nicht gezielt in Mitgliedsländern der EU und des EWR anbietet.

Zusätzlich kann die DSGVO zur Anwendung kommen, wenn absichtlich das Verhalten einer Person beobachtet wird, die sich in einem Mitgliedsland der EU aufhält. Eine Verhaltensbeobachtung liegt vor, wenn Internetaktivitäten mit Hilfe von Trackingtools erfasst und nachvollzogen werden, so dass aus den erhobenen Daten ein Nutzerprofil erstellt werden kann. Solche Verhaltensbeobachtungen haben beispielsweise zum Ziel, personalisierte Werbung zuzustellen. Doch auch hier ist die DSGVO für die städtische Verwaltung kaum von Relevanz. Bereits gestützt auf das Datenschutzrecht des Kantons Zürich ist der Stadtverwaltung die Nutzung von Tracking- und Analyse-Tools nur erlaubt, sofern deren Auswertung keine Rückschlüsse auf einzelne Personen zulassen.

FOKUS

Entwicklung des Datenschutzrechts

Keine praktische Relevanz für die Stadtverwaltung

Die Kriterien zur Bestimmung der Anwendbarkeit der DSGVO sind primär auf private Unternehmen und nicht auf die öffentliche Verwaltung zugeschnitten. Daher erstaunt es nicht, dass die DSGVO für die Stadtverwaltung weder aufgrund des Niederlassungsprinzips noch aufgrund des Markortprinzips von Bedeutung ist. Die Datenschutzstelle hat den Anwendungsbereich der DSGVO mit einzelnen Dienstabteilungen konkret geprüft und anschliessend die Stadtverwaltung mit einer entsprechenden Mitteilung im städtischen Intranet (Datenschutz-News) informiert. Bis anhin ist kein Fall bekannt, bei dem die DSGVO für die Stadtverwaltung zur Anwendung gekommen wäre. Somit haben sich die anfänglich hohen Wellen, die durch das Inkrafttreten der DSGVO ausgelöst wurden, wieder geglättet. Nichtsdestotrotz bleiben viele Fragen offen und die kommenden Jahre werden auch für die Stadtverwaltung zeigen, ob und allenfalls wie die DSGVO angewendet und ausgelegt werden muss.

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 erhöhtem 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 Personalossier.

Mit jeder Nutzung von E-Mail, Internet, Telefonie, elektronischen Schlüsseln oder GPS an städtischen Arbeitsplätzen fallen sogenannte Verkehrs- oder Logdaten an. Diese sind regelmässig notwendig, damit die technischen Infrastrukturen sicher und zuverlässig betrieben werden können. Damit ist aber auch die Möglichkeit der [Überwachung am Arbeitsplatz](#) grösser geworden. Solche Überwachungen sind nur in Ausnahmefällen und in engen Grenzen zulässig. Über allfällige Nutzungen von Verkehrs- oder Logdaten müssen die Angestellten ausreichend informiert werden. Wichtig ist deshalb die [Schaffung von Transparenz](#) und allenfalls auch von internen Regelungen.

FOKUS

Personalbereich

Im Personalwesen der Stadtverwaltung werden einige Aufgaben zentral durch die Dienstabteilung Human Resources Management (HRZ), andere dezentral durch die Dienstabteilungen erfüllt. In Zusammenhang mit Datenbearbeitungssystemen zeigt sich, dass die Zuordnung von **Zuständigkeit und Verantwortung** nicht immer einfach und klar ist.

Zum Fokus *Personalbereich* stellen wir aus dem Berichtsjahr zwei Beispiele vor. Das erste betrifft das vom Stadtrat erlassene Reglement über das mobile Arbeiten, das zweite den Trend, Personal-dossiers vermehrt digital zu führen.

Mobiles Arbeiten

Die Angestellten der Stadt Zürich haben die Möglichkeit, einen Teil ihrer Arbeit mobil und somit ausserhalb ihres üblichen Arbeitsplatzes zu erledigen. Das städtische Personalrecht kennt das mobile Arbeiten dem Grundsatz nach bereits seit einiger Zeit, detailliertere Bestimmungen dazu fehlten aber bislang. Der Stadtrat hat deshalb im Berichtsjahr ein Reglement über mobiles Arbeiten ausarbeiten lassen und dieses per Juni 2018 in Kraft gesetzt.

Bei der Erarbeitung des städtischen Reglements zum mobilen Arbeiten war auch die Datenschutzstelle involviert. Aus Sicht des Datenschutzes gab es dabei mehrere relevante Aspekte zu berücksichtigen:

Zuständigkeit und Verantwortung

Mobiles Arbeiten ist ein Zusammenspiel mehrerer Beteiligter – der Dienstabteilungen, die ihren Angestellten mobiles Arbeiten ermöglichen, der OIZ (Organisation und Informatik Stadt Zürich), die sich um die städtische Informatik-Basisinfrastruktur und um Belange der Informationssicherheit zu kümmern hat sowie der Angestellten, die mobil arbeiten. Werden Informationen durch mehrere Stellen oder Personen bearbeitet, stellen sich regelmässig Fragen nach Zuständigkeit und Verantwortlichkeit der jeweiligen Beteiligten. Die Datenschutzstelle legte besonderes Augenmerk darauf, dass sich das Reglement diesbezüglich genügend klar und verbindlich äussert.

Organisatorische Massnahmen

Das Reglement enthält gleich mehrere organisatorische Massnahmen, die zum Schutz der Informationen beitragen sollen.

Eignungsprüfung: Die Dienstabteilungen haben gemäss Reglement für jedes mobile Arbeiten zu prüfen, ob sich diese Arbeitsform im konkreten Fall eignet. Anhand eines Kriterienkatalogs wird den verantwortlichen Stellen ein Hilfsmittel für die verlangte Eignungsprüfung zur Verfügung gestellt. Unterteilt nach Tätigkeit, Person und Arbeitsort wird dabei auch auf datenschutzrechtlich relevante Kriterien hingewiesen, beispielsweise auf die Vertraulichkeit der zu bearbeitenden Informationen oder auf die Sachkenntnis und Sensibilisierung der Mitarbeitenden im Umgang mit sensiblen Informationen.

Bewilligung und schriftliche Vereinbarung: Zusätzlich zur Eignungsprüfung verlangt das Reglement, dass mobiles Arbeiten in jedem Fall bewilligt wird. Bei bloss gelegentlichem mobilen Arbeiten genügt eine Bewilligung durch die Vorgesetzten. Soll das mobile Arbeiten regelmässig stattfinden, bedarf es einer schriftlichen Vereinbarung mit den jeweiligen Angestellten, die auch Vorgaben zur Gewährleistung der Vertraulichkeit beinhalten muss.

Information und Schulung: Städtische Angestellte unterstehen dem Amtsgeheimnis und haben im Umgang mit Informationen und Personendaten Geheimhaltungs- und Sorgfaltspflichten zu beachten. Beim mobilen Arbeiten gelten diese Pflichten in erhöhtem Masse, da sich insbesondere in Bezug auf die Vertraulichkeit weitere Risiken als am Arbeitsplatz im Büro ergeben können. Die Dienstabteilungen haben deshalb gemäss Reglement mit den Angestellten nicht nur die erwähnten Vereinbarungen abzuschliessen, sondern auch dafür

zu sorgen, dass die Angestellten im Zusammenhang mit mobilem Arbeiten die Risiken und das richtige Verhalten kennen.

Technische Massnahmen

Mobil gearbeitet werden darf nur, wenn die Informationssicherheit gewährleistet ist. Das Reglement sieht deshalb vor, dass mobile Zugriffe auf städtische Informationen ausschliesslich nach den Vorgaben der OIZ erfolgen dürfen. Die Einhaltung dieser Vorgabe ist Bedingung für die erwähnte Bewilligungserteilung. Die von der OIZ für mobiles Arbeiten zur Verfügung gestellten Geräte, Infrastrukturen und Services stellen sicher, dass nur über verschlüsselte Verbindungen auf dienstliche Informationen zugegriffen werden kann. Die städtischen Angestellten müssen sich für den Zugriff auf diese Informationen über sogenannte 2-Faktor-Authentifizierungen anmelden. Sie brauchen also nebst Login und Passwort einen zusätzlichen Code, der ihnen vor jeder Anmeldung auf ihr Handy zugestellt wird. Auch unterstützen die Geräte, Infrastrukturen und Services der OIZ die Angestellten darin, vertrauliche Informationen ausschliesslich auf städtischen ICT-Infrastrukturen zu speichern.

Fazit

Nach Abschluss der Arbeiten der interdisziplinären Arbeitsgruppe konnte die Datenschutzstelle dem Stadtrat gegenüber festhalten:

1. Das Reglement bietet eine transparente und verständliche Grundlage für das mobile Arbeiten.
2. Die wesentlichen datenschutzrechtlichen Anliegen sind im Reglement angemessen berücksichtigt.

Digitales Personaldossier

Im Tätigkeitsbericht 2016 stellte die Datenschutzstelle die diversen Rechtsfragen dar, die sich im Zusammenhang mit der Führung digitaler Dossiers, insbesondere Personaldossiers, stellen. Im Berichtsjahr setzte sich die Datenschutzstelle nun mit der Umsetzung des digitalen Personaldossiers auseinander. Mit der Fachapplikation «aconso» stellt der zentrale städtische Personaldienst (HRZ) den Personalabteilungen der einzelnen Dienstabteilungen eine Datenablage zur Verfügung, welche die technische Infrastruktur für das digitale Führen von Personaldossiers – das sogenannte e-Dossier – schafft.

Verantwortlichkeit für die Daten

HRZ stellt die Applikation «aconso» den Dienstabteilungen nicht nur zur Verfügung, sondern bearbeitet auch selber bestimmte Daten in diesem System. Mit andern Worten greifen sowohl HRZ als auch die Personalabteilungen der Dienstabteilungen über diese zentrale Fachapplikation auf die darin vorhandenen Daten der städtischen Angestellten zu. Die Klärung der Verantwortlichkeiten und Zuständigkeiten in Bezug auf die Personaldaten war deshalb zentral. Es galt insbesondere zu klären, welche Daten in die alleinige Verantwortlichkeit der Dienstabteilungen und welche in diejenige von HRZ fallen und bei welchen allenfalls eine geteilte beziehungsweise doppelte Verantwortlichkeit vorliegt. Denn nur wenn transparent ist, wer für welche Daten und Dokumente verantwortlich ist, ist erkennbar, wer diese bearbeiten darf.

Aufbewahrungsdauer und Löschung der Personaldaten

Die Klärung der Verantwortung ist auch für die Löschung von Daten von Relevanz. Dokumente innerhalb eines Personaldossiers, die nicht mehr aktuell sind oder nicht mehr benötigt werden, sind zu löschen. Für diese Löschung ist die verantwortliche Dienstabteilung zuständig. Die digitale Erfassung der Daten bietet die Möglichkeit, für jedes Dokument ein Erstellungs- oder Ablagedatum zu erfassen und für bestimmte Dokumentarten eine maximale Aufbewahrungsdauer zu hinterlegen. Nach Ablauf der hinterlegten Aufbewahrungsdauer werden die Dokumente automatisch in einen Löschorner verschoben, welcher periodisch geleert wird.

Regelung der Zugriffsrechte

Die Dienstabteilungen, die die digitale Ablage für Personaldossiers nutzen, müssen nachvollziehen können, wer auf welche Daten ihrer Mitarbeiterinnen und Mitarbeiter zugreifen und diese bearbeiten kann. Als Inhaber der Fachapplikation «aconso» war HRZ zuständig für die Erstellung eines Berechtigungskonzepts. Das erstellte Konzept beschreibt die Kategorien der vorhandenen Daten sowie die dazugehörigen rollenbasierten Zugriffsrechte. Dieses Konzept ist für alle Dienstabteilungen verbindlich. Es wurde von der Datenschutzstelle auf dessen Vereinbarkeit mit dem Personalrecht, aber auch dessen Schlüssigkeit geprüft und für gut befunden.

Leitfaden Elektronisches Personaldossier

HRZ hat für die Führung digitaler Personaldossiers einen Leitfaden erstellt. In diesem werden verschiedene technische, rechtliche und organisatorische Fragen geklärt, die sich in diesem Zusammenhang regelmässig stellen. Die Datenschutzstelle begrüsst im Sinne der geforderten Transparenz die Verabschiedung dieses verständlichen Leitfadens. Dieser ermöglicht es den Dienstabteilungen, allfällige Fragen oder Unklarheiten im Zusammenhang mit dem digitalen Personaldossier zu klären und befähigt sie, kompetent eine Entscheidung pro oder contra e-Dossier im Personalbereich zu fällen.

FOKUS

Videüberwachung

Die Stadt Zürich hat für Videoüberwachungen der städtischen Verwaltungsstellen eigene gesetzliche Regelungen in der [städtischen Datenschutzverordnung](#) erlassen. Diese Verordnung sieht vor, dass die Stadtverwaltung Videoüberwachung an neuralgischen Punkten mit erheblicher Gefahr für Leib, Leben oder Sachen 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.

FOKUS

Videüberwachung

Die Beratungen zum Thema Videüberwachung und die Prüfung von Videoreglementen beanspruchen die Datenschutzstelle in besonderem Masse. Um welche Beratungen und Prüfungen es sich im Berichtsjahr handelte, erwähnen wir gleich anschliessend.

Im Kapitel [Feststellungen und Beurteilungen](#) ziehen wir zu den Videobestimmungen der Datenschutzverordnung Bilanz. Die Datenschutzstelle kommt zum Schluss, dass einige davon überprüft und allenfalls angepasst werden sollten.

Beratungen und Prüfungen im Bereich

Videüberwachung

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

Aktuell haben 12 städtische Dienstabteilungen Videoüberwachungen gestützt auf die Datenschutzverordnung der Stadt Zürich im Einsatz. Für die hierfür erstellten Reglemente ergab sich aufgrund der kürzlich stattgefundenen Revision der städtischen Publikationsvorschriften Anpassungsbedarf. Bei 4 Reglementen sind diese Arbeiten mittlerweile abgeschlossen. Diese sind in der Amtlichen Sammlung der Stadt Zürich publiziert. Es sind dies die Reglemente der Dienstabteilungen Stadtpolizei, Organisation und Informatik, Stadtspital Triemli und Museum Rietberg. Bei den restlichen Reglementen sind die Revisionsarbeiten noch im Gange.

Zusätzlich zu den 12 städtischen Dienstabteilungen, die bereits Videoüberwachung im Einsatz haben, sind im Berichtsjahr 3 weitere dazugekommen, die neu Videoüberwachung einsetzen wollen und hierfür Reglemente erstellen. Auch diese Arbeiten sind noch im Gange und finden in Zusammenarbeit mit der Datenschutzstelle statt.

Im anschliessenden Kapitel [Feststellungen und Beurteilungen](#) werden diese Arbeiten und insbesondere die Schwierigkeiten und Herausforderungen, die sich in diesem Zusammenhang stellen, näher beschrieben.

Anfragen Privater zu Videüberwachung

Im Berichtsjahr meldeten sich rund 30 Privatpersonen bei der Datenschutzstelle mit Fragen oder Anliegen zu Videüberwachung. Sämtliche Anfragen betrafen Videüberwachungen, für die nicht die Stadtverwaltung, sondern Private verantwortlich waren. Von den fraglichen Videüberwachungen war in vielen Fällen auch öffentlicher Grund der Stadt Zürich (mit)betroffen.

Für Videüberwachungen 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. Zuständig für Beratung und Aufsicht bei Videüberwachung durch Private ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB). Sofern derartige Anfragen bloss mit einer allgemeinen Rechtsauskunft beantwortet werden können, erteilt die Datenschutzstelle gerne Auskunft. Bei allen übrigen Anfragen muss die Datenschutzstelle die anfragenden Personen aus Zuständigkeitsgründen jeweils an den EDÖB weiterverweisen.

Motion GR Nr. 2017/63; Erweiterung der Beratungsaufgaben der Datenschutzstelle

Mit dieser Motion sollen die Beratungsaufgaben der Datenschutzstelle erweitert werden. Zukünftig soll die Datenschutzstelle auch bei Videüberwachungen durch Privatpersonen Beratungen anbieten, sofern diese Videüberwachungen öffentlichen Grund der Stadt Zürich tangieren. Die Motion ist bis September 2019 umzusetzen. Die Datenschutzstelle wurde in die diesbezüglichen Arbeiten miteinbezogen. Zurzeit befindet sich die Motion im Vernehmlassungsverfahren.

Feststellungen und Beurteilungen

Videüberwachung

Anlass zu Feststellungen und Beurteilungen in Zusammenhang mit Videüberwachung ergibt sich für die Datenschutzstelle aus zweifacher Hinsicht: Einerseits deshalb, weil per Januar 2018 die revidierten Publikationsvorschriften der Stadt Zürich in Kraft getreten sind. Diese Vorschriften wirken sich unmittelbar auch auf die städtischen Videobestimmungen aus. Andererseits weil die mittlerweile 8-jährige Praxiserfahrung zeigt, dass verschiedene Bestimmungen zur Videüberwachung in der Datenschutzverordnung nicht genügend klar sind.

1. Die städtische Publikationsverordnung und ihre Auswirkungen auf die Videüberwachung

Die Publikationsverordnung der Stadt Zürich regelt die amtliche Veröffentlichung von Erlassen und Beschlüssen der städtischen Behörden und Verwaltung. Sie verlangt, dass rechtsetzende Erlasse im Amtsblatt zu veröffentlichen und anschliessend in die Amtliche Sammlung aufzunehmen sind. Im Rahmen der erwähnten Revision der Publikationsverordnung beschloss die Stadt Zürich, zukünftig neu auch Videoreglements in die Amtliche Sammlung aufzunehmen, die von öffentlichem Interesse sind. Damit erhalten diese Videoreglements eine hohe Publizität und sind für Interessierte einfacher zugänglich. Die Transparenz über die Videüberwachung wird damit erhöht, was aus datenschutzrechtlicher Sicht sehr zu begrüssen ist. Der Entscheid, auch Videoreglements zukünftig in die Amtliche Sammlung aufzunehmen, wirkt sich aber auch in anderer Hinsicht direkt auf diese aus. Die wesentlichen Auswirkungen sind folgende:

Unterscheidung nach öffentlichem und nicht öffentlichem Raum

Die Datenschutzverordnung verlangt für jede Videoüberwachung mit Bild- oder Tonaufzeichnung ein Reglement. In die Amtliche Sammlung aufgenommen werden können aber nur Videoreglements, die öffentlichen beziehungsweise allgemein zugänglichen Raum betreffen und somit von öffentlichem Interesse sind. Videoüberwachungen, die nicht öffentlichen oder nicht allgemein zugänglichen Raum betreffen, beispielsweise in Gebäuden oder auf Geländen, wo nur städtische Angestellte Zutritt haben, sind (bloss) verwaltungsinterne Angelegenheiten. Sie tangieren die Öffentlichkeit nicht, weshalb die diesbezüglichen Reglements nicht amtlich publiziert werden können. Zahlreiche Dienstabteilungen haben Videoüberwachungen im Einsatz, die sowohl öffentlichen als auch nicht öffentlichen Raum betreffen. Dies bringt mit sich, dass bei solchen Konstellationen nebst den amtlich publizierten und in die Amtliche Sammlung aufgenommenen auch noch verwaltungsinterne Reglements erlassen werden müssen. Diese «Doppelspurigkeit» und der damit verbundene Aufwand werden sich nicht vermeiden lassen.

Abstraktionsgrad der Videoreglements

Mit der Datenschutzverordnung wurde die Reglementsspflicht eingeführt, um Transparenz über den Einsatz von Videoüberwachung zu schaffen. Im damaligen Gesetzgebungsverfahren vor rund zehn Jahren wurde davon ausgegangen, dass die Dienstabteilungen die erforderlichen Videoreglements ohne grösseren Aufwand erstellen und bei Bedarf rasch anpassen können. Ob und gegebenenfalls wie die Videoreglements zu veröffentlichen sind, war damals kein Thema.

Mit der Aufnahme in die Amtliche Sammlung erhalten die Videoreglements nun einen anderen «Charakter». Sie werden zu eigentlichen Rechtserlassen. Das hat zur Folge, dass die Videoreglements weniger rasch und flexibel angepasst werden können und vermehrt in generell-abstrakter Weise formuliert werden müssen. Gleichzeitig werden die Reglements auch weiterhin die Aufgabe haben, die Bevölkerung über die Videoüberwachung zu informieren. Es gilt deshalb, ein Gleichgewicht zwischen Abstraktionsgrad und genügender Transparenz zu finden. Dies führt konkret zu folgenden Herausforderungen:

- **Beschreibung der Bereiche, die von der Videoüberwachung erfasst werden**

In früheren Reglements wurde der räumliche Bereich, der von der Videoüberwachung erfasst wird, oft in separaten Anhängen und zum Teil unter Angabe jeder einzelnen Kamera ausgewiesen. Mit der Aufnahme der Reglements in die Amtliche Sammlung müssen diese Bereiche allgemeiner beschrieben werden. Wichtig ist, dass die jeweiligen erfassten Bereiche dennoch soweit konkret und aussagekräftig beschrieben werden, dass erkennbar ist, an welchen Orten eine Videoüberwachung erfolgt. Dies ist beispielsweise der Fall bei Beschreibungen wie «Hauseingang innen», «Lift» oder «Treppenhaus» bei konkret genannten Amtsgebäuden. Nicht der Fall wäre dies bei einer zu pauschalen Beschreibung, beispielsweise in der Art von «Innenbereich Gebäude». Bei den Anforderungen an die Beschreibung der erfassten Bereiche ist mit zu berücksichtigen, dass jede Videoüberwachung auch vor Ort erkennbar sein muss, was mit Piktogrammen oder Hinweisschildern geschieht.

- **Beschreibung der organisatorischen und technischen Sicherheitsmassnahmen**

Die Datenschutzverordnung verlangt, dass im Reglement auch die organisatorischen und technischen Sicherheitsmassnahmen beschrieben werden. Es hat sich gezeigt, dass Beschreibungen von konkreten Massnahmen in den Videoreglementen wenig praktikabel sind, da sowohl organisatorische als auch technische Belange regelmässig überprüft und angepasst werden müssen. Im Zusammenhang mit dem Beschrieb von Sicherheitsmassnahmen in Videoreglementen stellt sich nicht nur die Frage der Praktikabilität, sondern auch des Erfordernisses an sich: Aus Sicht der betroffenen Personen ist es massgebend, dass die Stadt Zürich für die Videoüberwachung genügende Sicherheitsmassnahmen verlangt und deren Einhaltung überprüft. Dies ist bereits mit den bestehenden kantonalen und städtischen Vorschriften zur Informationssicherheit, welche auch für Videoüberwachungen verbindlich sind, der Fall. Es stellt sich deshalb die Frage, welchen (Mehr-)Wert ein abstrakt gehaltener Beschrieb von Sicherheitsmassnahmen in allen Videoreglementen für die betroffenen Personen bringen kann.

- **Regelung der Zugriffsrechte, der Einsichtnahme und der Auswertung**

Die Videoreglemente haben die Zugriffsrechte, die Einsichtnahme und die Auswertung zu regeln. In diesem Zusammenhang stellt sich regelmässig die Frage, ob und wie detailliert in den Videoreglementen auch dienstabteilungsinterne Abläufe oder Zuständigkeiten beschrieben werden müssen. So wie Sicherheitsmassnahmen sind auch interne Abläufe und Zuständigkeiten wenig geeignet, in Rechtserlassen festgeschrieben zu werden, da sich diese rasch ändern können.

2. Die Datenschutzverordnung der Stadt Zürich

Die Datenschutzverordnung enthält zahlreiche Bestimmungen zur Videüberwachung, sowohl in inhaltlicher als auch in formeller Hinsicht. Bei folgenden Regelungen zeigen sich in der Praxis regelmässig Unklarheiten:

Voraussetzungen der Videüberwachung

Die städtische Datenschutzverordnung stellt hohe Anforderungen an den Einsatz von Videüberwachung durch die Stadtverwaltung. Zulässig ist eine Videüberwachung nur an *«neuralgischen Punkten mit erheblicher Gefahr für Leib, Leben oder Sachen»*. Gemäss Wortlaut der städtischen Datenschutzverordnung gilt diese hohe Hürde für alle Videüberwachungen.

In der Praxis wird diese Regelung bei «harmlosen» Videüberwachungen als wenig praktikabel und nicht sachgerecht empfunden. Dies kann der Fall sein bei Videüberwachungen ohne Aufzeichnung. Selbstverständlich können auch Videüberwachungen ohne Aufzeichnung sensibel sein, so insbesondere, wenn damit eine eigentliche Verhaltensüberwachung geschieht oder wenn sie an Orten erfolgt, an welchen eine solche Überwachung üblicherweise nicht zu erwarten ist. Es gibt aber auch immer wieder Konstellationen, bei welchen eine Videüberwachung ohne Aufzeichnung die Persönlichkeit betroffener Personen kaum oder gar nicht tangiert. So beispielsweise bei sogenannten «Türspionen», bei welchen Bilder auf einen Bildschirm übertragen werden, sobald jemand an der Tür klingelt. Es stellt sich die Frage, ob die Messlatte der erheblichen Gefahr für Leib, Leben und Sachen auch für Videüberwachungen so hoch anzusetzen ist, bei welchen keine Bilder aufgezeichnet

Videüberwachung

werden und die aus Sicht Privats- und Persönlichkeitssphäre als nicht sensibel zu bewerten sind.

Aus dem damaligen parlamentarischen Gesetzgebungsprozess der Jahre 2010 und 2011 geht hervor, dass der Gemeinderat keine Videoüberwachung für die Ahndung geringfügiger Delikte oder Bagatellfälle erlauben wollte. Ob der Gemeinderat auch Videoüberwachungen ohne Aufzeichnung und ohne besondere datenschutzrechtliche Relevanz nur unter den erwähnten strengen Voraussetzungen zulassen wollte, geht daraus nicht klar hervor.

Nach Ansicht der Datenschutzstelle sollte – wie bei allen Datenbearbeitungen – auch bei der Videoüberwachung der allgemeine datenschutzrechtliche «Massstab» angewendet werden: Die Voraussetzungen und Anforderungen im Umgang mit Personendaten richten sich nach deren Sensibilität und Grundrechtsrelevanz. Bringt eine Bearbeitung von Personendaten keinen oder nur einen marginalen Eingriff in die Persönlichkeit Betroffener mit sich, sind dementsprechend auch keine erhöhten Voraussetzungen und Anforderungen zu verlangen. Eine diesbezügliche Klärung durch den Gesetzgeber wäre zu begrüssen.

Die Verwendung von Videoaufzeichnungen

Die Datenschutzverordnung sieht vor, dass Videoaufzeichnungen nur zur Geltendmachung zivil- und strafrechtlicher Ansprüche eingesehen und verwendet werden dürfen. Diese Regelung wurde insbesondere mit Blick auf die Videoüberwachung im Schulbereich eingeführt. Es sollte ausgeschlossen werden, dass im Schulbetrieb Schülerinnen und Schüler mit Videokameras überwacht werden. Mittlerweile hat sich gezeigt, dass diese Regelung für andere Verwaltungsbereiche zu einschränkend ist. Nach Ansicht der Datenschutzstelle sollte sich auch die Verwendung der Aufzeichnungen nach dem jeweiligen Zweck der Videoüberwachung auszurichten haben.

3. Fazit

Nach Einschätzung der Datenschutzstelle hat es sich bewährt, dass der städtische Gesetzgeber die Videoüberwachung durch die Stadtverwaltung mit Voraussetzungen, einer Reglementsspflicht sowie einer Prüfungspflicht durch die Datenschutzstelle reglementiert. Zahlreiche dieser Regelungen haben sich denn auch in der Praxis bewährt. Dennoch besteht nach Ansicht der Datenschutzstelle Bedarf, einzelne Videobestimmungen in der städtischen Datenschutzverordnung zu überprüfen, insbesondere hinsichtlich Zulässigkeit der Videoüberwachung und Verwendung von Aufzeichnungen. Die Aufnahme der Videoreglements in die Amtliche Sammlung wirkt sich wie erwähnt in mehrfacher Hinsicht auf die Videoreglements aus. Ausgehend vom Informations- und Transparenzbedürfnis der Bevölkerung im Zusammenhang mit Videoüberwachung ist zu prüfen, welche Informationen in die Reglements der Amtlichen Sammlung aufzunehmen sind und welche Informationen von den zuständigen Dienstabteilungen zusätzlich dazu besser in anderer Weise zur Verfügung zu stellen sind.

Städtisches Zugangsportal

«Mein Konto»

Wer die Webseite der Stadtverwaltung Zürich besucht, kann den Link auf «Mein Konto» nicht übersehen. Einen Klick weiter erfährt man, dass es sich bei «Mein Konto» um den zentralen Zugang zu den Online-Services der Stadt Zürich handelt. Viele Behördengänge sollen damit bequem und jederzeit online erledigt werden können. So können beispielsweise Umzüge gemeldet, Schul-, Betreuungs- oder Ferienangebote für Kinder gebucht, Parkkarten gekauft oder Steuererklärungen eingereicht werden. Das Angebot wird laufend erweitert.

«Mein Konto» startete vor rund vier Jahren. Zum damaligen Zeitpunkt konnte noch nicht genau definiert werden, wie das städtische Zugangsportale auszusehen und über welche Funktionalitäten dieses zu verfügen hat. Mit jeder Einbindung von Online-Services aus den Dienstabteilungen der Stadtverwaltung entwickelte sich «Mein Konto» weiter. Ähnliches galt auch in Bezug auf die Anliegen des Datenschutzes. Erst mit der Einbindung konkreter Online-Services zeigte sich, welche datenschutzrechtlichen Anforderungen zu erfüllen und welche Massnahmen zu verlangen sind. Die Datenschutzstelle prüfte «Mein Konto» deshalb auch im Berichtsjahr jeweils Schritt für Schritt, das heisst immer dann, wenn weitere städtische Online-Services eingebunden wurden.

Mittlerweile hat sich «Mein Konto» zu dem digitalen Zugang zu Online-Services der Stadtverwaltung und damit zu einer eigenständigen städtischen Plattform oder Infrastruktur entwickelt. Um sicherzustellen, dass mit den Daten der Benutzerinnen und Benutzer von «Mein Konto» auch weiterhin korrekt umgegangen wird, bedarf es zusätzlicher organisatorischer Massnahmen. Vereinfacht gesagt gilt

es, Klarheit und Verbindlichkeit hinsichtlich der wichtigsten datenschutzrechtlichen Grundsätze und Spielregeln zu schaffen. Dies betrifft insbesondere folgende Themen:

- *Verantwortungen und Zuständigkeiten:* Bei «Mein Konto» sind regelmässig mehrere städtische Verwaltungsstellen involviert, insbesondere die Dienstabteilung Organisation und Informatik (OIZ) als Betreiberin von «Mein Konto» und die Dienstabteilungen, die einen Online-Service in «Mein Konto» einbinden. Die Verantwortungen und Zuständigkeiten für die jeweiligen Services und Daten sind deshalb zu regeln.
- *Informationelle Trennung innerhalb der Stadtverwaltung:* Es muss sichergestellt sein, dass Dienstabteilungen nur Zugang zu denjenigen Informationen haben, die ihre eigenen Serviceangebote betreffen.
- *Informationelle Selbstbestimmung:* Die Benutzerinnen und Benutzer müssen soweit wie möglich selber bestimmen können, welche Informationen sie in welcher Weise in «Mein Konto» bearbeiten wollen.
- *Persönliche Ablage:* Wenn mit «Mein Konto» auch die Möglichkeit angeboten wird, persönliche Daten zu speichern, müssen die hierfür wichtigsten Modalitäten wie Aufbewahrungsdauer, Löschfristen oder Zugriffsrechte bekannt sein.
- *Konto- und Stammdaten:* Der Zweck dieser Daten über die Benutzerinnen und Benutzer, der Zugang dazu und deren Verwendung für die einzelnen Serviceangebote müssen verbindlich geregelt werden.
- *Datenportabilität:* Zu klären ist, inwieweit persönliche Informationen aus «Mein Konto» auf andere Plattformen oder Datenträger übertragbar sein sollen.
- *Transparenz:* Benutzerinnen und Benutzer sind transparent und verständlich über «Mein Konto» zu informieren.

Städtisches Zugangsportal «Mein Konto»

Die Datenschutzstelle hat im Berichtsjahr der zuständigen Dienst-
abteilung OIZ und dem Finanzdepartement mitgeteilt, dass das Zu-
gangsportal «Mein Konto» zukünftig nicht mehr nur auf Konzepten,
Handbüchern und Dokumenten der OIZ basieren darf. In Anbetracht
der Bedeutung von «Mein Konto» sowohl für die Bevölkerung als
auch die gesamte Stadtverwaltung muss der Stadtrat die wich-
tigsten Grundsätze und Prinzipien des städtischen Zugangsportals
vorgeben.

Interview

Die städtischen Beraterinnen und Berater für Datenschutz

Die Stadt Zürich kennt seit über 20 Jahren die Funktion der Beraterinnen und Berater für Datenschutz. In allen Departementen der Stadtverwaltung ist eine Juristin oder ein Jurist des Rechtsdienstes Ansprechperson für Datenschutzbelange der jeweiligen Dienstabteilungen und Verwaltungsstellen. Die Beraterinnen und Berater für Datenschutz der Departemente beraten und informieren ihre Dienstabteilungen und arbeiten regelmässig mit der Datenschutzstelle zusammen.

[Simone Thür](#), Beraterin für Datenschutz des Präsidialdepartements, und [Robert Soos](#), Berater für Datenschutz des Sicherheitsdepartements, beantworten die Fragen der Datenschutzstelle. Sie verfügen beide über langjährige Erfahrung in dieser Funktion.

Das Datenschutzrecht gibt es in der Schweiz seit über 25 Jahren. Wie nehmen Sie das Thema Datenschutz in der Stadtverwaltung heute wahr? Sind die Mitarbeitenden sensibilisiert für dieses Thema? Wie gehen sie damit um?

[Soos](#): Zu Beginn meiner Tätigkeit als Berater für Datenschutz hatte die Stadtverwaltung das Thema eher wenig auf dem Radar. Zwischenzeitlich hat sich das aber stark geändert. Nach meiner Wahrnehmung wissen die Mitarbeitenden, dass sie bei ihrer Arbeit dem Datenschutz die notwendige Aufmerksamkeit schenken müssen.

[Thür](#): Ich bin nun seit fünf Jahren in dieser Funktion bei der Stadt und stelle auch eine Zunahme von Anfragen respektive eine höhere Sensibilisierung bei den Mitarbeitenden fest. Allerdings habe ich manchmal den Eindruck, dass das Thema «Datenschutz» teilweise

Die städtischen Beraterinnen und Berater für Datenschutz

instrumentalisiert wird. Je nachdem, ob die Wahrung des Datenschutzes der eigenen Zielsetzung gerade dient oder nicht, wird er stärker oder weniger stark gewichtet.

Welche Datenschutz-Themen beschäftigen die Stadtverwaltung?
Gibt es Dauerthemen, die immer wieder für Gesprächsstoff sorgen?

Soos: Der Einsatz von Videogeräten ist ein Dauerbrenner. Die Politik, die Medien und auch die Bevölkerung sind am Thema sehr interessiert. Das ist verständlich, sind wir doch alle davon betroffen, wenn die Verwaltung Videotechnik einsetzt. Durch die rasante technische Entwicklung mit der Digitalisierung vieler Geschäftsprozesse sind auch datenschutzrechtliche Fragen zu klären, Stichworte sind da beispielsweise IT-Sicherheit oder Zugriffsbeschränkungen.

Thür: Interessant, in unserem Departement haben wir erst per 1. April 2019 die ersten Videokameras installiert, nämlich im Museum Rietberg zur Sicherung der Kunst- und Archivgegenstände. Ein wichtiges Thema ist bei uns die stadtinterne Datenbekanntgabe aus dem Einwohnerregister des Bevölkerungsamts, insbesondere über die elektronische Datenplattform OMEGA. Den Dienstabteilungen wird auf ihr Gesuch hin unter bestimmten Voraussetzungen die Online-Abfrage über OMEGA bewilligt. Dabei gilt es sicherzustellen, dass eine Dienstabteilung lediglich die Daten erhält, die sie zur Erfüllung ihrer gesetzlichen Aufgaben auch tatsächlich benötigt.

Welche Schwierigkeiten gibt es bei der Umsetzung des Datenschutzes in der Verwaltung?

Thür: Projekte müssen teilweise angepasst werden, damit sie datenschutzrechtlichen Anforderungen genügen, das kann als Hemmnis empfunden werden.

Die städtischen Beraterinnen und Berater für Datenschutz

Soos: Datenschutz gibt es nicht umsonst. Als Verwaltung muss man bereit sein, Arbeit und Zeit zu investieren, um die datenschutzrechtlichen Rahmenbedingungen zu erfüllen. Das kann eine Herausforderung sein, wenn in einem Geschäft oder Projekt zeitlicher Druck besteht.

Zur Funktion der Datenschutz-Beraterinnen und -Berater: Wie beurteilen Sie den Wert dieser Funktion? Braucht es diese Funktion auch weiterhin?

Soos: Ich glaube, dass die Funktion zwischenzeitlich als wertvoll angesehen und geschätzt wird. Als Berater für Datenschutz nehme ich nicht selten eine Art Scharnierfunktion zwischen der Datenschutzstelle und den Dienstabteilungen wahr, indem ich den Kontakt herstelle, Verständnis für die unterschiedlichen Anliegen schaffe oder ein Geschäft koordiniere. Alles in allem ist die Beraterfunktion auch ein Beitrag zu mehr Effizienz.

Thür: Das sehe ich auch so. Der Datenschutz bildet eine Schnittstelle, an der Mitarbeitende aus verschiedenen Abteilungen und Bereichen miteinander zu tun haben und unterschiedliche Sprachen sprechen. Die Beraterin für Datenschutz ist häufig in der Rolle der «Übersetzerin». Ich finde es sinnvoll, wenn die Funktion weiterhin besteht und der Austausch über die Departemente hinaus gepflegt wird.

Als Juristin oder Jurist im Rechtsdienst von städtischen Departementen haben Sie vielfältige Aufgaben zu erfüllen. Die Funktion als Beraterin oder Berater für Datenschutz ist nur eine von mehreren. Kann es da zu Interessenkonflikten kommen?

Thür: Es gehört allgemein zur Funktion als Departementsjuristin, zwischen unterschiedlichen Interessen innerhalb eines Departements abzuwägen unter Berücksichtigung der rechtlichen und politischen

Die städtischen Beraterinnen und Berater für Datenschutz

Rahmenbedingungen. Es geht darum, den grössten gemeinsamen Nenner zu finden, das gilt auch im Bereich Datenschutz.

Soos: Persönlich würde ich nicht von Interessenkonflikten sprechen. Es geht vielmehr darum, die einzelnen öffentlichen Interessen zu gewichten und Lösungen zu finden, die der Verwaltung, dem Datenschutz und letztlich der Bevölkerung dienen.

Als Beraterin oder Berater für Datenschutz arbeiten Sie auch mit der städtischen Datenschutzstelle zusammen. Was kann man sich darunter vorstellen? Und wie beurteilen Sie diese Zusammenarbeit?

Soos: Die Datenschutzstelle ist eine sehr verlässliche Ansprechpartnerin. Sie nimmt die Aufgaben und Anliegen der Stadtverwaltung ernst und versucht ausnahmslos, konstruktive Lösungen zu finden. Dies kann bei grösseren Gesetzgebungsarbeiten der Fall sein, aber auch bei kleineren Fragestellungen. Eine gewisse Hartnäckigkeit ist dem Datenschutzbeauftragten nicht abzusprechen, wenn es um seinen Fachbereich geht – aber das muss so sein und ist selbstverständlich zu respektieren.

Thür: Dem kann ich zustimmen. Die Datenschutzstelle ist sehr lösungsorientiert und interessiert sich für die spezifischen Anliegen der Departemente. Sie legt den Datenschutz sehr praxisbezogen aus und nicht dogmatisch. Ich schätze auch den regelmässigen Austausch im Gremium der Beraterinnen und Berater. Der Wissens- und Erfahrungsaustausch führt zu einer einheitlichen Handhabung von datenschutzrechtlichen Themen in der Stadtverwaltung.

Im Berichtsjahr setzte sich die Fachstelle
Datenschutzbeauftragter personell wie folgt
zusammen:

Marcel Studer, RA lic. iur.

Wirtschaftsinformatiker NDS
Datenschutzbeauftragter (80%)

Patrizia Zbinden, Dr. iur.

juristische Mitarbeiterin (80%)

Katrin Gisler, MLaw

juristische Mitarbeiterin (80%)

Jürg von Flüe, lic. iur.

juristischer Mitarbeiter (60%)

Monika Niederberger

Sekretariat (20%)

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