Stadt Zürich
Datenschutzbeauftragter

Tätigkeitsbericht 2012

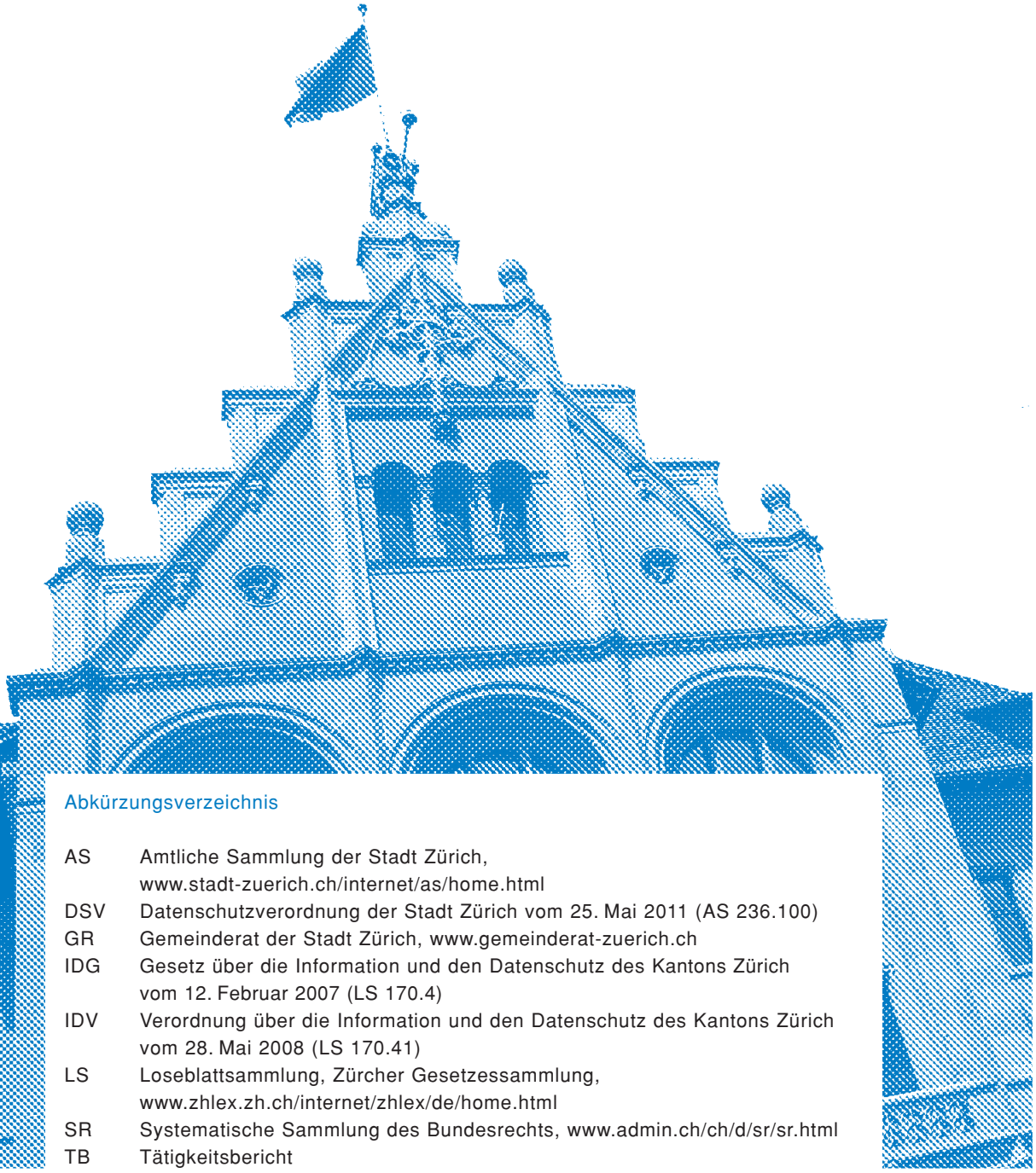
Der Datenschutzbeauftragte hat dem Gemeinderat jährlich einen Bericht über Tätigkeit und Feststellungen und über den Stand des Datenschutzes zu erstatten*.

Der vorliegende Tätigkeitsbericht deckt den Zeitraum von 1. Januar 2012 bis 31. Dezember 2012 ab.

Der Bericht ist abrufbar unter www.stadt-zuerich.ch/datenschutz.

*§ 39 IDG

Inhaltsverzeichnis



Abkürzungsverzeichnis

AS	Amtliche Sammlung der Stadt Zürich, www.stadt-zuerich.ch/internet/as/home.html
DSV	Datenschutzverordnung der Stadt Zürich vom 25. Mai 2011 (AS 236.100)
GR	Gemeinderat der Stadt Zürich, www.gemeinderat-zuerich.ch
IDG	Gesetz über die Information und den Datenschutz des Kantons Zürich vom 12. Februar 2007 (LS 170.4)
IDV	Verordnung über die Information und den Datenschutz des Kantons Zürich vom 28. Mai 2008 (LS 170.41)
LS	Loseblattsammlung, Zürcher Gesetzessammlung, www.zhlex.zh.ch/internet/zhlex/de/home.html
SR	Systematische Sammlung des Bundesrechts, www.admin.ch/ch/d/sr/sr.html
TB	Tätigkeitsbericht

I Berichtsjahr 2012

Das Schweizerische Datenschutzrecht hat das Erwachsenenalter erreicht. Rund 20-jährig sind die Datenschutzgesetze des Bundes und des Kantons Zürich, die Stadt Zürich hat ihre Datenschutzverordnung seit 15 Jahren. Dies ist Anlass dafür, dass derzeit viel über den Datenschutz nachgedacht und geschrieben wird[1] – sowohl mit Blick zurück, aber vor allem auch nach vorne schauend. Wo stehen wir heute mit unserer Datenschutzgesetzgebung in der Schweiz? Hat sich diese bewährt oder ist sie nur noch so nützlich wie eine rostige Flinte?[2] Hat der Gesetzgeber das Steuer angesichts der Entwicklungen in den Informations- und Kommunikationstechnologien überhaupt noch in der Hand?

Die Meinungen, Erwartungen und Vorschläge zur Zukunft des Datenschutzrechts fallen wie bei jedem anderen gesellschaftlichen und rechtlichen Thema unterschiedlich aus. Einigkeit besteht insoweit, als dass wir uns weder heute noch morgen in einer Post-Privacy-Zeit befinden (wollen), in der Werte wie Privatsphäre oder Datenschutz bedeutungslos werden oder anachronistisch anmuten. Um es nicht soweit kommen zu lassen, wird sich auch das Datenschutzrecht weiterentwickeln und anpassen müssen.

Zur Diskussion stehen unter anderem Zielsetzungen wie früheres Eingreifen des Datenschutzes (privacy by design), verstärkte Sensibilisierung, Erhöhung der Transparenz, Verbesserung der Datenkontrolle und -herrschaft oder Schutz von Minderjährigen.[3] Es werden vor allem die Gesetzgebungen von Bund und Kantonen sein, die auf die technischen und gesellschaftlichen Entwicklungen reagieren und entsprechend fortentwickelt werden müssen. Die Handlungsspielräume und Einflussmöglichkeiten auf städtischer Ebene werden dabei zwar beschränkt sein, eine Neuausrichtung im Datenschutz wird aber auch auf kommunaler Ebene unmittelbare Auswirkungen haben. Dies gilt beispielsweise in Bezug auf die Forderung, die Datenschutzgesetzgebung in Bund und Kantonen zu vereinheitlichen, so dass die Schweiz nur noch ein Datenschutzgesetz haben würde. Eine Vereinheitlichung der datenschutzrechtlichen Grundsätze und Prinzipien ist unseres Erachtens ein sinnvoller Ansatz und wäre wohl keine allzu schwierige Angelegenheit, unterscheiden sich doch bereits heute die diversen Datenschutzgesetze in der Schweiz diesbezüglich nur unwesentlich. Die grössere Herausforderung wird dann aber die Frage sein, welche Aufsichtskompetenzen den Datenschutzstellen der drei Staatsebenen bei einer derartigen Rechtsvereinheitlichung zustehen sollen. Diskutiert wird nämlich auch eine Anpassung in dem Sinne,

[1] Bspw. der Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335 ff. [2] Brunner Stephan C., Mit rostiger Flinte unterwegs in virtuellen Welten?, in: Jusletter 4. April 2011. [3] FN 1, Ziff. 5.2.2.

dass die Aufsichtsaufgaben (zumindest in bestimmten Fällen) auch im Privatbereich an die kantonalen Aufsichtsbehörden delegiert werden könnten, weil diese mit lokalen Verhältnissen besser vertraut sind.[4] Ob das gleiche Argument dann auch im Verhältnis von kantonaler und städtischer Aufsichtsstelle zum Tragen kommen soll, wird sich erst noch zeigen. Eine föderalistische Zuteilung der Aufsichtsaufgaben im öffentlichen Bereich macht Sinn und hat sich bewährt, denn massgebend für die Informationsbearbeitungen durch die (kantonalen und kommunalen) Verwaltungen ist in erster Linie das kantonale und kommunale Bereichsrecht wie bspw. das Polizei- oder Sozialhilferecht. Wenig Sinn macht unseres Erachtens aber eine Dezentralisation der Aufsichtskompetenzen im Privatbereich. Privatrecht ist Bundessache und als solche einer Bundesaufsicht zu unterstellen.

Wie die künftigen Entwicklungen des Datenschutzrechts auf nationaler und kantonaler Ebene auch aussehen werden, sicher ist, dass die Stadt Zürich als kommunale Verwaltung unmittelbar am Puls der Zeit und für die Umsetzung zahlreicher Aufgaben auf zeitnahe Lösungen angewiesen ist. Die nachfolgend erwähnten Beispiele aus dem Berichtsjahr der Datenschutzstelle veranschaulichen dies.

[4] FN 2, Rz 23/24.

II Themen

1 Videoüberwachung

Immer mehr Gebäude und Liegenschaften werden videoüberwacht. Was möglich ist und was nicht, hält die Datenschutzverordnung fest, die im Oktober 2011 in Kraft getreten ist. Was haben die gesetzlichen Anforderungen für Konsequenzen?

Seit dem Inkrafttreten der Datenschutzverordnung (DSV) am 1. Oktober 2011 müssen Videoüberwachungen den gesetzlichen Anforderungen in Art. 9 und 10 DSV genügen. Für alle Videoüberwachungen müssen Berichte erstellt werden, die das Vorliegen dieser gesetzlichen Voraussetzungen darlegen, und meistens ist auch ein Reglement zu erstellen[5]. Für Videoüberwachungen, die zum Zeitpunkt des Inkrafttretens der DSV bestanden, wurde eine Übergangsfrist von einem Jahr, das heisst bis zum 30. September 2012, festgelegt (Art. 20 Abs. 2 DSV).

Obwohl die Datenschutzstelle alle Datenschutzberaterinnen und -berater der Departemente, Dienstchefinnen und Dienstchefs sowie Departementssekretariate früh informierte, zeichnete sich bald ab, dass die einjährige Übergangsfrist gerade für umfangreichere Videoüberwachungen zu knapp war. Bis zum Stichtag konnten nur einzelne Videoüberwachungen abschliessend auf ihre Vereinbarkeit mit den gesetzlichen Bestimmungen geprüft – und deshalb nur wenige Reglemente in Kraft gesetzt und publiziert – werden.

Zum einen stellte sich heraus, dass die Zuständigkeit für die Erstellung der Reglemente geklärt werden musste. Unklar war, ob eine Dienstabteilung als Mieterin oder die Liegenschaftenverwaltung (IMMO) als Bewirtschafterin der Verwaltungsgebäude das Reglement erstellen musste. Nach internen Abklärungen ist grundsätzlich die IMMO für die Reglemente in Gebäuden oder Liegenschaften zuständig, die sie bewirtschaftet. Haben die Videoüberwachungen vor allem betriebliche Gründe, beispielsweise in Hallenbädern oder Sportanlagen, müssen die IMMO und die Betreiberin bei der Ausarbeitung der Berichte und Reglemente eng zusammenarbeiten. Keine Reglemente müssen die Verkehrsbetriebe der Stadt Zürich erlassen, da für diese Videoüberwachungen Bundesrecht gilt[6].

Zum anderen liegen die Gründe darin, dass das Verfahren zeitaufwändig ist und Einige den Aufwand unterschätzt haben. So müssen zuerst alle Kameras beziehungsweise überwachten Örtlichkeiten erfasst werden. Dazu gehören neben der Qualifikation als Videoüberwachung mit oder ohne Bild- und Tonaufzeichnung auch die Beschreibung des überwachten Ortes

[5] Ausführende Informationen wie Ablaufschema, Erläuterungen zum Bericht und ein Muster-Reglement mit Erläuterungen sind online unter www.stadt-zuerich.ch/datenschutz, «Informationen für Stadtverwaltung», abrufbar. [6] Bundesverordnung über die Videoüberwachung im öffentlichen Verkehr, SR 742.147.2.

sowie die Erfassung der Überwachungszeiten und aller von der Überwachung betroffenen Personen.

Im Bericht muss für die einzelnen Videoüberwachungen, die unter Umständen in Kategorien wie Amtshäuser oder Pflege- und Altersheime zusammengefasst werden können, dargelegt und begründet werden, dass die Voraussetzungen laut Art. 9 Abs. 1 DSV («erhebliche Gefahr für Leib, Leben oder Sachen», «an neuralgischen Punkten») vorliegen und die Videoüberwachung verhältnismässig ist. Die Datenschutzstelle berät und unterstützt die Dienstabteilungen regelmässig in dieser frühen Phase, weil die Übersicht über die Kameras und die Ausführungen in den Berichten die Voraussetzung und Grundlage für die Ausarbeitung der Reglemente sind.

In Einzelfällen haben die verantwortlichen Stellen Mühe, das Vorliegen der gesetzlich verlangten Voraussetzungen in Art. 9 Abs. 1 DSV und die Verhältnismässigkeit bei allen Kameras gleichermassen klar darzulegen. Das Problem dieser Stellen liegt darin, bestehende und geplante Videoüberwachungen mit den neuen gesetzlichen Voraussetzungen unter einen Hut zu bringen. Gelingt das nicht oder nicht ganz, bedeutet dies, dass von bisherigen Videoüberwachungen zumindest teilweise abgesehen werden muss.

Die Datenschutzstelle hat in diesem Zusammenhang immer wieder daran erinnert, dass sich der Gemeinderat der Stadt Zürich für eine restriktive Handhabung ausgesprochen und die Hürde für Videoüberwachungen der Stadtverwaltung hochgelegt hat. Fehlen die gesetzlichen Voraussetzungen gemäss Art. 9 Abs. 1 DSV, können auch restriktive Regeln wie kurze Aufbewahrungszeiten oder strenge Zugriffsregelungen daran nichts ändern.

Die Datenschutzstelle geht davon aus, dass die bei ihr noch hängigen Verfahren in den nächsten Monaten erledigt werden können. Eine erste repräsentative Aussage über Einsatz und Ausmass von Videoüberwachungen durch die Stadtverwaltung sollte Ende 2013 möglich sein.

2 REID[7]

Mitarbeitende können und sollen E-Mail und Internet während der Arbeit auch privat nutzen dürfen. Die Spielregeln hält das neue Reglement über die Nutzung elektronischer Infrastrukturen oder Dienste der Stadt Zürich fest.

Die Vorgeschichte

Die Datenschutzstelle berichtete bereits in ihrem Tätigkeitsbericht 2010 darüber, dass das «Reglement über die Nutzung und Überwachung von Internet und E-Mail» durch ein umfassenderes Reglement ersetzt werden sollte, das die Nutzung elektronischer Infrastrukturen (wie PC, Telefongeräte, Drucker) oder Dienste (wie Internet oder E-Mail) unabhängig vom (mobilen) Endgerät regelt. Seit Anfang 2010 arbeitete eine Gruppe aus Vertreterinnen und Vertretern aus dem Departementssekretariat des Finanzdepartements, Human Resources Management Stadt Zürich und Organisation und Informatik der Stadt Zürich unter der Leitung des Datenschutzbeauftragten an einem neuen Reglement. Das neue Reglement baut auf dem überarbeiteten städtischen Internet- und E-Mail-Reglement auf und orientiert sich an den auf Bundesebene am 1. April 2012 neu in Kraft getretenen Bestimmungen, die das «Bearbeitung von Personendaten bei der Nutzung der elektronischen Infrastruktur»[8] in der Bundesverwaltung regeln.

Nachdem der Stadtrat die Vorlage am 11. April 2012 provisorisch beschlossen hatte, wurde sie den Departementen und Dienstabteilungen, der Konferenz der Schulpräsidentinnen und Schulpräsidenten sowie den Personalverbänden zur Vernehmlassung bis Mitte Juli 2012 vorgelegt. Im Vernehmlassungsverfahren wurde der Vorschlag einhellig begrüsst. Bestimmungen, die in materieller Hinsicht kritisiert worden waren, hat die Arbeitsgruppe anschliessend überarbeitet. Dazu zählten unter anderem die Bestimmungen zur Kostenregelung, die Aufzählung der Aufzeichnungszwecke sowie die zu eng gefasste Formulierung möglicher personenbezogener Auswertungen von Verkehrsdaten. Der Stadtrat hat das REID per 1. Juli 2013 in Kraft gesetzt und gleichzeitig das bisherige Internet- und E-Mail-Reglement aufgehoben.

Das neue REID

Wie erwähnt wird der Geltungsbereich des Internet- und E-Mail-Reglements auf alle elektronischen Infrastrukturen oder Dienste der Stadt Zürich ausgeweitet. Der Zweck der Reglementierung bleibt derselbe: Das Reglement soll die gesetzliche Grundlage für das Bearbeiten bestimmter Personendaten, so genannter Verkehrsdaten, durch die Stadt Zürich schaffen und die Nutzerinnen und Nutzer umfassend über Rechte und Pflichten und allfällige Sanktionen bei Widerhandlungen informieren.

[7] REID = Reglement über die Nutzung elektronischer Infrastrukturen oder Dienste der Stadt Zürich. [8] Art. 57i ff. des Eidgenössischen Regierungs- und Verwaltungsorganisationsgesetzes, RVOG, SR 172.010.

Das REID regelt vor allem die private Nutzung und den Missbrauch elektronischer Infrastrukturen oder Dienste der Stadt Zürich. Dazu zählen der Umgang mit E-Mails sowie die Zugriffsrechte auf personalisierte Ablagen wie das persönliche E-Mail-Konto, persönliche E-Mail-Ablagen und -Archive oder das in der Regel private Laufwerk «H».

Neu regelt das REID auch die Kostenübernahme durch die Mitarbeitenden. Bisher waren die Gebühren für private Telefongespräche in einem Stadtratsbeschluss (Deklarationspflicht für Privatgespräche) geregelt. Diese Regelung ist wegen der technologischen Entwicklungen überholt und musste überarbeitet werden: Die Dienstabteilungen haben die Abrechnungen zu kontrollieren und die Kosten, die durch eine missbräuchliche oder übermässige private Nutzung elektronischer Infrastrukturen oder Dienste verursacht werden, ihren Mitarbeitenden in Rechnung zu stellen.

Geregelt werden schliesslich auch personenbezogene Auswertungen von Verkehrsdaten. Solche sind – unter bestimmten Voraussetzungen und Bedingungen – «bei Störungen», «bei Zugriffen auf Datensammlungen», «bei Verdacht auf Missbrauch», «bei strafbaren Handlungen» und «zu weiteren Zwecken» zulässig. Auswertungen «zu weiteren Zwecken» setzen allerdings voraus, dass die Departementsvorstehenden diese Auswertungen vorgängig in einem Reglement konkretisieren und für ihre Mitarbeitenden transparent machen.

Wie beim Erlass des Internet- und E-Mail-Reglements hat der Stadtrat Human Resources Management der Stadt Zürich beauftragt, alle städtischen Mitarbeitenden vorgängig über Inkrafttreten, Inhalt und Anwendung des neuen Reglements zu informieren.

3 E-Health

Im Berichtsjahr wurden in beiden Stadtspitälern verschiedene E-Health-Projekte lanciert. Die Projekte sollen zu einer Vereinfachung, Beschleunigung und Qualitätsverbesserung der Behandlungsabläufe beitragen.

Bei E-Health-Projekten spielt der Datenschutz eine zentrale Rolle, da in der Regel komplexe Schnittstellen zu spitalinternen Patienteninformationssystemen notwendig sind, neue Technologien eingesetzt oder Patienteninformationen mit spitalexternen Ärzten ausgetauscht werden. Die Datenschutzstelle berät alle involvierten Stellen und prüft im Rahmen der Vorabkontrolle die Einhaltung aller datenschutzrechtlichen Rahmenbedingungen. Neben spezifschen rechtlichen Fragen (wie dem Patientengeheimnis) müssen wegen der Sensibilität der Daten insbesondere die Anforderungen an die Informationssicherheit genau geklärt und die notwendigen Massnahmen bestimmt und überprüft werden. In diesem Bereich arbeitet die Datenschutzstelle eng mit den IT-Security-Fachleuten der OIZ und der Stadtspitäler zusammen. Bei E-Health-Projekten muss immer im Auge behalten werden, dass alle an der Behandlung eines Patienten beteiligten spitalinternen und -externen Fachleute (wie Ärzte, Pflegefachpersonen oder Physiotherapeuten) in unterschiedlichem Umfang und mit unterschiedlicher zeitlicher Dringlichkeit auf Patienteninformationen angewiesen sind.

Stadtspital Waid: Hausärzte greifen online auf Patientenberichte zu

Das Stadtspital Waid hat die Zusammenarbeit mit den Hausärzten intensiviert. Als erstes Spital im Kanton Zürich hat es für Hausärzte, die Patientinnen und Patienten dem Spital zuweisen, ein so genanntes Zuweiserportal realisiert[9]. Die Medien haben darüber ausführlich berichtet[10]. Seit Juli 2012 können die Hausärzte Patientendaten wie Röntgenbilder oder Operations- und Austrittsberichte online einsehen sowie mittels E-Mail-Versand als PDF zugestellt erhalten und sie so direkt in ihr elektronisches Patienteninformationssystem übernehmen. Diese Neuerungen haben für zuweisende Ärzte den Vorteil, dass sie schneller Zugriff auf aktuelle Patienteninformationen erhalten und die anschliessende Nachbehandlung einfacher wird.

(Datenschutz-)Rechtlich liegt der zentrale Ansatzpunkt für E-Health-Projekte beim Patientengeheimnis. Grundsätzlich bestimmt der Patient, welche persönlichen Daten das Spital den zuweisenden Ärzten weitergeben darf. Spricht sich ein Patient gegen den Informationsaustausch aus, müssen die Spitalärzte das respektieren. Zu beachten ist jedoch, dass die an der Behandlung beteiligten Hausärzte auf Patienteninformationen angewiesen sind. Deshalb sieht das Patientinnen- und Patientengesetz des Kantons Zürich vor,

[9] Das Stadtspital Triemli hat mit der Realisierung eines vergleichbaren Projektes begonnen.
[10] Bspw. Tages-Anzeiger vom 29. November 2012.

dass das Spital vor- oder nachbehandelnde Ärzte über den Gesundheitszustand ihrer Patientinnen und Patienten und weitere notwendige Massnahmen rechtzeitig orientiert, ausser, eine Patientin oder ein Patient spricht sich explizit dagegen aus[11], was in der Praxis aber nur ganz selten geschieht.

Was die Gewährleistung der Informationssicherheit betrifft, war bei diesem Projekt sicherzustellen, dass nur berechtigte Hausärzte Zugang zu den Daten ihrer Patienten erhalten. Deshalb wird das Zuweiserportal über HIN (Health Info Net), die im Schweizerischen Gesundheitswesen grösste E-Health Plattform (www.hin.ch) mit fortschrittlicher Verschlüsselungs- und Authentifizierungstechnologie, betrieben. Ausserdem können nur jene Spitalärzte, welche medizinisch verantwortlich sind, bestimmen, welche Patienteninformationen den zuweisenden Ärzten bekannt und somit für den Onlinezugang oder elektronischen Versand frei zu geben sind.

Stadtspital Triemli: Patienten werden mit RFID-Technologie geortet

Mit dem Pilotprojekt RFID-Patiententracking ist die in der Logistikbranche weit verbreitete RFID-Technologie (radio-frequency identification) auch im Stadtspital Triemli eingeführt worden. Die Patientinnen und Patienten erhalten dabei ein elektronisches Armband mit einem RFID-Tag. Im Rahmen des Pilotprojekts ist der Einsatz des Patiententrackingsystems auf das Ambulante Perioperative Zentrum (APZ)[12] beschränkt. Bereits heute wird im APZ zur Steuerung der Behandlungsprozesse ein Patientenleitsystem eingesetzt, mit dem die Standorte aller Patienten von Hand mit Zeitangabe erfasst werden. Das RFID-Patiententracking soll diese Aufgaben automatisieren.

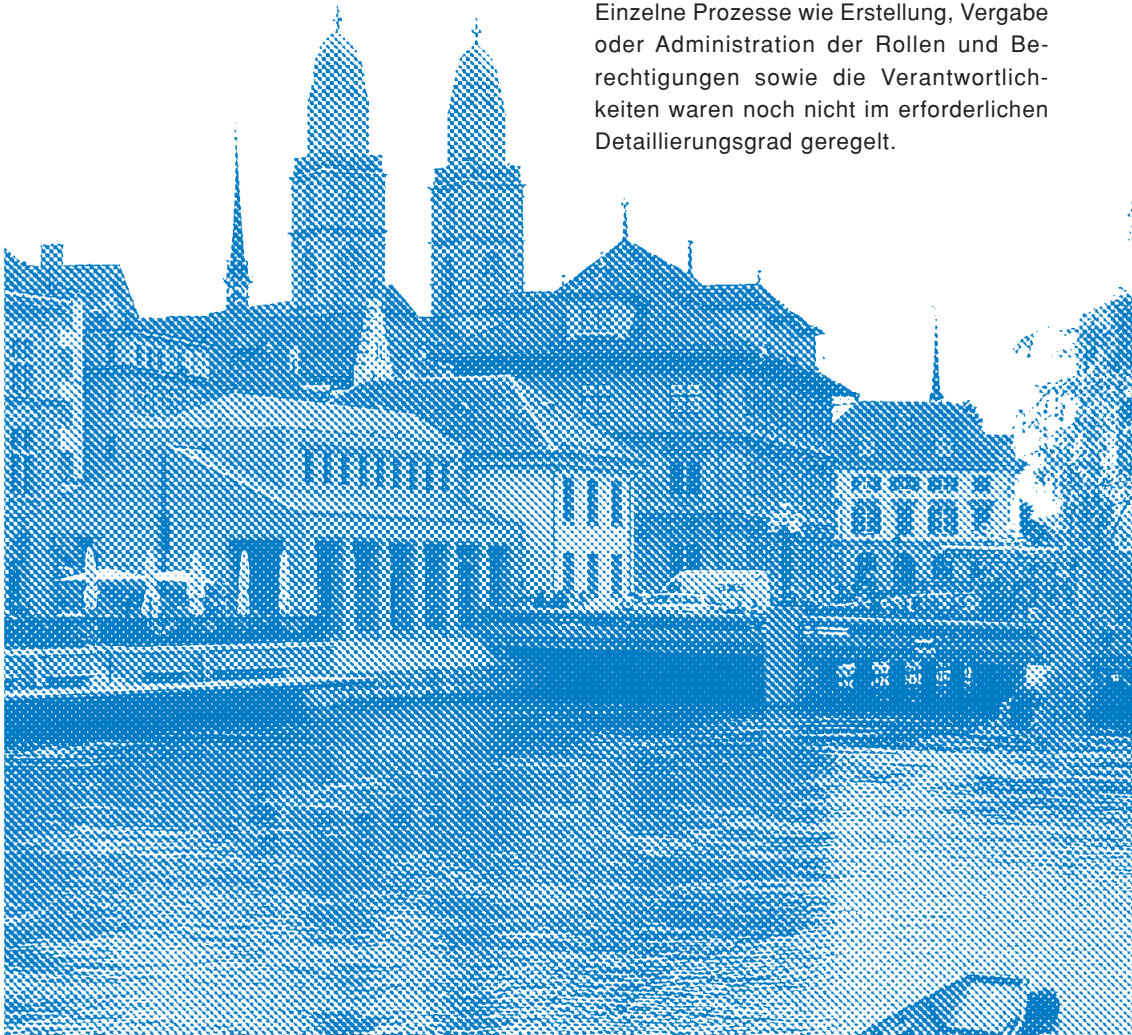
Aus datenschutzrechtlicher Sicht zeigen sich im Pilotprojekt keine besonderen Schwierigkeiten. Einerseits ist auf dem elektronischen Armband mit RFID-Tag nur eine Nummer gespeichert, die für Dritte keinen Informationswert hat. Andererseits ist die Ortung auf die Zugangs- und Behandlungsbereiche im APZ beschränkt. In allen anderen Bereichen bewegen sich die Patienten, ohne geortet zu werden. Eine allfällige Ausweitung des Patiententrackings wird eine erneute Überprüfung der datenschutzrechtlichen Fragen nach sich ziehen.

Stadtspital Triemli: Patienteninformationssystem für den Pflegedienst

Patientinnen und Patienten werden in Spitälern nicht nur durch Ärztinnen und Ärzte, sondern genauso durch Pflegerinnen und Pfleger betreut. Für den ärztlichen Dienst setzt das Stadtspital Triemli schon lange ein elektronisches Patienteninformationssystem[13] ein. Im Pflegedienst stand bisher kein elektronisches System zur Verfügung. Pflegerinnen und Pfleger mussten ihre Arbeit handschriftlich dokumentieren.

Mit dem Projekt «PflegIS» ist nun ein elektronisches Pflegedokumentationssystem realisiert worden.

Die Datenschutzstelle hat das Projekt im Rahmen einer Vorabkontrolle geprüft und gestützt auf das Informationssicherheits- und Datenschutzkonzept und den positiven Bericht der IT-Security OIZ grundsätzlich grünes Licht erteilt. Die Datenschutzstelle verlangte allerdings eine Nachbesserung beziehungsweise Vervollständigung des Zugriffs- und Berechtigungskonzepts. Einzelne Prozesse wie Erstellung, Vergabe oder Administration der Rollen und Berechtigungen sowie die Verantwortlichkeiten waren noch nicht im erforderlichen Detaillierungsgrad geregelt.



[11] § 16 Patientinnen- und Patientengesetz; LS 813.13. [12] Dieses interdisziplinär ausgerichtete Zentrum übernimmt vor operativen Eingriffen die Koordination aller medizinischen Informationen und führt entsprechende Untersuchungen durch. [13] Vgl. TB 2003, S.11.

4 Zurich by App

Auf Smartphones und Tablets sind sie nicht mehr wegzudenken: Applikationen, die auf Fingerdruck Wichtiges und Nützliches bereitstellen. Auch die Stadtverwaltung nutzt Apps, um Informationen oder Dienstleistungen schnell und zeitgemäss an den Mann und die Frau zu bringen. Die Datenschutzstelle war in zwei Projekte involviert.

«Silvesterzauber»

Besucherinnen und Besucher des Silvesterzaubers 2012 konnten eine kostenlose Smartphone-App herunter laden, mit der sie den Festplan, das Programm und weitere Informationen abfragen konnten. Die App fragte die Nutzerinnen und Nutzer nach der Installation, ob sie damit einverstanden seien, dass ihre Smartphones via GPS-Technologie lokalisiert werden, wenn sie die App nutzen, und diese Informationen der ETH Zürich für ein Forschungsprojekt zur Verfügung gestellt werden. Ziel dieses Projektes war es, über Geolokalisierung und die Bestimmung von Verhaltensmustern die Bewegungen von Menschenströmen antizipieren zu können. Solche Projekte sind die Grundlage, um Frühwarnsysteme zu entwickeln für Gefahren, die von grossen Menschenansammlungen ausgehen (Crowd Management). Beteiligt war auch die Stadtpolizei Zürich. Sie erhielt von der ETH Zürich animierte Grafiken und Übersichten, sogenannte Heat-maps, die zum einen die Dichte und zum anderen die Bewegungen einzelner Menschenansammlungen sichtbar machten.

Um eine möglichst grosse Teilnahme am Forschungsprojekt zu erreichen, war es wichtig, bei den App-Nutzenden Vertrauen zu schaffen, dass ihre persönlichen Daten datenschutzkonform bearbeitet werden. Die Stadtpolizei Zürich bat deshalb die Datenschutzstelle, das Projekt zu prüfen.

Untersucht wurden alle Informationen, die mit Einwilligung der App-Nutzenden von den Smartphones an die ETH übermittelt wurden (1), die Informationsbearbeitung bei der ETH zu Forschungszwecken (2) sowie die Bekanntgabe von Informationen durch die ETH an die Stadtpolizei Zürich (3). Da die ETH Zürich ein Bundesorgan ist, das dem Datenschutzgesetz des Bundes unterliegt, erfolgte die Prüfung der ersten zwei Informationsbearbeitungen auf Wunsch der städtischen Datenschutzstelle in Zusammenarbeit mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Die App «Silvesterzauber» erfüllte alle datenschutzrechtlichen Anforderungen. Auch wurde den Empfehlungen der Datenschutzstellen entsprochen, welche mit der Installation ausreichende und verständliche Informationen forderten, damit sich App-Nutzende in gültiger Weise zu einer Teilnahme am Forschungsprojekt einverstanden erklären konnten. Aus Sicht Stadtverwaltung war massgebend, dass die Stadtpolizei zu keinem Zeitpunkt im Besitz von datenschutzrechtlich relevanten Daten war, weil die ihr zur Verfügung gestellten Grafiken und Übersichten keine Rückschlüsse auf Personen ermöglichten.

Gemäss Medienmitteilung der Stadtpolizei Zürich wurde die App rund 2700 Mal herunter geladen. Für die Forschenden habe die App wertvolle Grundlagen geliefert. Für die Stadtpolizei hätten sich aber wegen der geringen Benutzung und der Überlastung der Netze keine direkt brauchbaren Resultate ergeben.

«Züri wie neu»

Über die Webseite oder die App «Züri wie neu» können Mängel an der Infrastruktur der Stadt Zürich unkompliziert gemeldet werden. Mit wenigen Angaben, Klicks und eventuell einem Foto können Schadensmeldungen schnell an die Stadtverwaltung übermittelt werden. Eingehende Meldungen werden geprüft und anschliessend zusammen mit Antworten und Statusmeldungen der Stadtverwaltung veröffentlicht.

Die Dienstabteilung Geomatik + Vermessung der Stadt Zürich unterbreitete das Vorhaben der Datenschutzstelle zur Prüfung. Auch bei dieser App-Anwendung konnte die Datenschutzstelle feststellen, dass die datenschutzrechtlichen Anforderungen eingehalten werden. So sind insbesondere die persönlichen Angaben der Personen, die eine Meldung machen, auf ein Minimum beschränkt. Mit der Meldung muss nur eine E-Mail-Adresse und optional ein Name oder eine Telefonnummer angegeben werden. Die Meldungen werden ohne persönliche Informationen zu Verfasserin oder Verfasser veröffentlicht. Die persönlichen Angaben werden ausschliesslich für eine standardisierte Rückmeldung (per E-Mail) oder eine allenfalls erforderliche Rücksprache (Telefonnummer) verwendet. Ausserdem sind die Informationsbearbeitungen, Zuständigkeiten und Berechtigungen klar und nachvollziehbar geregelt. Die Informationssicherheit wurde durch die OIZ IT-Security geprüft und als ausreichend und angemessen beurteilt.

«Züri wie neu» startete im April 2013 und ist als Pilotprojekt für die Dauer von einem Jahr angelegt.

5 Cloud Computing

In der IT-Welt ist Cloud Computing hoch im Kurs. Daten, Anwendungen und Infrastrukturen auslagern ist auch für die Verwaltung ein Thema. Weil die meisten Cloud-Anbieter ihre Server im Ausland betreiben, sind die Ansprüche an die vertraglichen Vereinbarungen und die Datensicherheit besonders hoch.

Regelmässig bringt die Informations- und Kommunikationstechnologie neue Trends und Begriffe hervor. Einer aus der jüngsten Vergangenheit ist Cloud Computing. Gemeint ist die Bereitstellung enormer Rechen- und Speicherkapazitäten, die eine bedarfsgerechte Nutzung von Daten, Anwendungen oder Infrastrukturen über das Internet ermöglicht. Kunden von Cloud-Anbietern profitieren von höherer Flexibilität und Kostenersparnissen. Diesen Vorteilen stehen aber auch Risiken gegenüber: Da die Kapazitäten und Ressourcen aus vielen Einzelteilen bestehen und rund um den Globus verteilt sein können, ist es mitunter schwierig zu bestimmen, wo sich die «Wolke» befindet. Souveränität und Kontrolle über die eigenen Daten werden dadurch nicht nur eingeschränkt, sondern unter Umständen vollends aufgegeben.

Rechtlich gesehen ist Cloud Computing kein neues Thema. Die Datenschutzgesetzgebungen sehen vor, dass Datenbearbeitung durch Dritte (Outsourcing) zulässig ist, sofern Daten nur so bearbeitet werden, wie es die verantwortliche Verwaltungsstelle selber auch tun dürfte und keine rechtlichen Bestimmungen dagegen sprechen. Dass es sich bei Cloud Computing um ein Outsourcing der besonderen Art handelt, zeigt sich unter anderem darin, dass der Steuerausschuss E-Government des Bundes im Oktober 2012 die «Cloud-Computing-Strategie der Schweizer Behörden 2012 – 2020» verabschiedet hat. Danach soll die Verwaltung für Daten und Anwendungen, die einem erhöhten Sicherheitsbedarf genügen müssen, dedizierte, von den Behörden kontrollierte Government-Cloud-Dienste nutzen, die in sogenannten Community-Clouds bereitgestellt werden.

Bis diese Vision der E-Government-Strategie Realität wird, ist es für die Verwaltung sehr beschränkt möglich, Cloud Computing zu nutzen. Die Nutzung wäre nur mit einer vertraglichen Regelung mit dem Cloud-Anbieter möglich, was wegen der inhaltlichen Anforderungen an die Regeln schwierig und komplex wäre. So müsste nebst der genauen Spezifikation von Auftrag und Haftung insbesondere sichergestellt werden, dass alle Sicherheitsmassnahmen gewährleistet sind, die Verwaltung ihre gesetzlichen Kontrollrechte jederzeit ausüben kann, alle datenschutzrechtlichen Anforderungen an Datenbearbeitungen im Ausland erfüllt sind und Schweizer Recht mit Schweizerischem Gerichtsstand für das Vertragsverhältnis gilt. Solche vertragliche Vereinbarungen sind mit weltweit tätigen Cloud-Anbietern kaum zu realisieren, da sie in der Regel nicht bereit sind, von ihren Standardverträgen abzuweichen.

Die vertraglichen Anforderungen waren auch der Grund, weshalb beim ersten und bisher einzigen Anwendungsfall, bei welchem die Datenschutzstelle beratend beigezogen wurde, keine Cloud-Vereinbarung zustande kam. Eine Dienstabteilung der Stadtverwaltung erwog, für ihr Beratungsangebot allenfalls Cloud-Dienstleistungen eines der weltweit grössten Anbieters in Anspruch zu nehmen. Die Daten wären im Ausland, vor allem in den USA, bearbeitet worden. Da der Cloud-Anbieter nicht bereit war, einen Dienstleistungsvertrag mit dem geforderten Regelungsinhalt abzuschliessen, verzichtete die Dienstabteilung auf ein externes Cloud-Computing.

6 Webportal eRente

Die Versicherten der Pensionskasse der Stadt Zürich sollen bald online ihre Daten abfragen und Mutationen melden können. Besonderes Augenmerk ist vor allem darauf zu legen, wer Einsicht in die Versicherteninformationen erhält.

Die Pensionskasse der Stadt Zürich (PKZH) zählt neben der Stadtverwaltung 150 Firmen, ungefähr 30'000 Versicherte und rund 16'000 Pensionsberechtigte zu ihren Kunden. Mit dem Webportal eRente sollen alle Kunden in Zukunft sicher und online Daten abfragen, Mutationen melden und Dokumente verschicken oder erhalten können. Die Versicherten haben ausserdem die Möglichkeit, mit ihren bei der PKZH gespeicherten Informationen ihre persönliche Rentensituation zu simulieren und ihre Rente zu berechnen.

Im Rahmen der durchgeführten Vorabkontrolle war aus rechtlicher Sicht das Einsichtsrecht der Stadt Zürich in die Pensionskasseninformationen ihrer Mitarbeitenden der wichtigste Prüfpunkt. Das Bundesgericht hat in einem Entscheid aus dem Jahr 2012[14] klargestellt, dass zahlreiche Informationen über die berufliche Vorsorge von Angestellten den Arbeitgebenden grundsätzlich nicht zugänglich sein dürfen. Das Bundesgericht musste prüfen, ob eine unverschlossene Weiterleitung von Pensionskassenausweisen durch den Arbeitgeber an seine Angestellten zulässig sei. Laut Bundesgericht lassen sich den Vorsorgeausweisen verschiedene Informationen entnehmen. Zum Beispiel, welche Freizügigkeitsleistungen neu eintretende Versicherte einbringen, wann und mit wie viel sich jemand in die Pensionskasse eingekauft hat, ob Pensionskassenguthaben für den Erwerb von Wohneigentum vorbezogen wurden, ob und wann sich das Guthaben eines Versicherten wegen einer Scheidung verändert hat oder auf wie viel sich die angesparten Pensionskassenguthaben belaufen. Unter Umständen befinden sich auch Hinweise auf den provisorischen Versicherungsschutz oder die temporäre Erwerbsunfähigkeit auf dem Vorsorgeausweis. Ausserdem wird jährlich die Höhe der Freizügigkeitsleistung bekannt gegeben. Gemäss Bundesgericht ist ein Arbeitgeber für diese Informationen der beruflichen Vorsorge als Drittperson zu qualifizieren, so dass eine Bekanntgabe nur zulässig ist, wenn eine rechtliche Grundlage gegeben ist. Eine solche ist aber nicht vorhanden und für das Bundesgericht ist auch kein Grund ersichtlich, weshalb die Arbeitgebenden Informationen aus Versicherungsausweisen brauchen, um ihre Pflichten im Rahmen der beruflichen Vorsorge oder im Rahmen des Arbeitsverhältnisses zu erfüllen.

Diese Erwägungen des Bundesgerichts und die daraus abgeleiteten Verpflichtungen betreffend die Zustellung von Pensionskassenausweisen sind auch unmittelbar auf das Zugriffsrecht für das Webportal anzuwenden, weil damit vergleichbare Informationen der beruflichen Vorsorge zur Verfügung gestellt werden. Die Datenschutzstelle hat in der Vorabkontrolle Wert darauf gelegt, dass die rechtlichen Grenzen des Einsichtsrechts der Arbeitgebenden in den Projektdokumentationen deutlich zum Ausdruck kommen und die Zugriffsregelung für das Webportal entsprechend realisiert wird. In diesem Zusammenhang ist auch die Schweigepflicht nach Art. 86 BVG wichtig: Würde die PKZH eine zu weitgehende Einsicht in Versicherungsdaten der städtischen Mitarbeitenden ermöglichen, würde sie ihre gesetzliche Schweigepflicht und die Persönlichkeitsrechte ihrer Versicherten verletzen.

Ein Zugriff auf vertrauliche Informationen verlangt zusätzlich nach entsprechenden technischen und organisatorischen Sicherheitsmassnahmen. Vor allem, wenn der Zugriff über ein Webportal erfolgen soll. Die vorgesehenen Sicherheitsmassnahmen wurden in der Vorabkontrolle geprüft. Gemäss Prüfbericht der OIZ IT Security wird allen relevanten Gefahren angemessen Rechnung getragen. Unter anderem mit einer starken Benutzerauthentifizierung, verschlüsselten Kommunikationskanälen, klar definierten Benutzerberechtigungen und dem Aufzeichnen aller Aktivitäten.

[14] Bundesgerichtsentscheid A-4467/2011 vom 10. April 2012.

7 Personenidentifikator

Informationen aus Datenbanken können dank Identifikatoren verknüpft und Personen oder Haushalten zugewiesen werden. Neben den Vorteilen für die effiziente Datenbearbeitung sind auch die Risiken im Auge zu behalten.

In Datenbanken werden häufig sogenannte Identifikatoren verwendet, um beispielsweise Personen anhand von Nummern eindeutig zu identifizieren. Solche Personenidentifikationsnummern verbessern Genauigkeit, Effizienz und Wirtschaftlichkeit der Datenbearbeitung. Diesen Vorteilen stehen aus Sicht des Datenschutzes aber Risiken gegenüber: So können Datensammlungen dank Personenidentifikationsnummern einfach verknüpft werden, was die Persönlichkeitsrechte der Betroffenen tangieren kann. Es liegt auf der Hand, dass mit der Anzahl Datenbanken, die mit demselben Personenidentifikator erschlossen und verknüpft werden können, die Gefahr zweckwidriger Auswertungen und missbräuchlicher Verwendungen von Personendaten steigen.

Die wohl wichtigste Identifikationsnummer ist die AHV-Versichertennummer. Mit der Revision des Bundesgesetzes über die Alters- und Hinterbliebenenversicherung (AHVG) im Dezember 2007 ist aus der einfachen AHV-Nummer eine systematisch verwendbare Sozialversicherungsnummer geworden. Ausserdem wurde mit der Revision das Fundament gelegt, damit die AHV-Versichertennummer als «administrative Personenidentifikationsnummer» verwendet werden kann. Bund und Kantonen ist es erlaubt, gesetzliche Grundlagen für die systematische Verwendung der AHV-Versichertennummer ausserhalb der Sozialversicherung und ohne thematische Einschränkung zu schaffen[15]. Es braucht dafür eine konkrete gesetzliche Ermächtigung auf Bundes- oder Kantonsebene.

Die erste gesetzliche Grundlage für die Verwendung als administrative Personenidentifikationsnummer wurde mit dem am 1. Januar 2008 in Kraft getretenen Registerharmonisierungsgesetz (RHG) geschaffen. Das Gesetz regelt den Einsatz der AHV-Versichertennummer in verschiedenen amtlichen Registern, unter anderem in kantonalen und kommunalen Einwohner- und Stimmregistern. Seither wurden weitere bereichsspezifische Rechtsgrundlagen um die Ermächtigung ergänzt, die AHV-Versichertennummer gemäss AHVG systematisch verwenden zu dürfen. Beispielsweise im ETH-Gesetz oder im Waffengesetz.

Auch in der Stadtverwaltung werden Identifikatoren und AHV-Versichertennummer verwendet, um Personen zu identifizieren. Die datenschutzrechtliche Beurteilung verlangt, den Blick nicht nur auf die Verwendung für die einzelne Aufgabenerfüllung zu richten, sondern auch eine Gesamtsicht einzunehmen und v.a. mögliche Konsequenzen, die sich aus weiteren Verknüpfungen ergeben können, nicht aus dem Auge zu verlieren.

AHV-Nummer für Lohnstatistik

Seit 1994 führt das Bundesamt für Statistik (BFS) bei den Arbeitgebern die Schweizerische Lohnstrukturerhebung durch. Dabei handelt es sich um eine schriftliche Stichprobenerhebung bei rund 49'000 privaten und öffentlichen Unternehmen beziehungsweise Verwaltungen mit insgesamt rund 1,9 Millionen Arbeitnehmenden (Stand 2010). Die Teilnahme ist obligatorisch. Die Arbeitgeber müssen anhand eines umfassenden Fragebogens detaillierte Informationen über ihre Angestellten liefern, zum Beispiel über Arbeitszeit, Anzahl Ferientage, Bruttolohn, Familienzulage und Sozialversicherungsbeiträge. Bisher erfolgte die Lohnstrukturerhebung vollständig anonymisiert, so dass Rückschlüsse auf einzelne Angestellte ausgeschlossen waren.

Mit der Lohnstrukturerhebung 2012 wurde die AHV-Nummer erstmals in die Erhebung miteinbezogen. Da mit der AHV-Nummer die Lohnstrukturdaten den einzelnen Angestellten zugeordnet werden können, ist die Erhebung auch datenschutzrechtlich sensitiv. Human Resources Management der Stadt Zürich (HRZ) bat die Datenschutzstelle zu beurteilen, ob die Erhebung der AHV-Nummer im Rahmen der Lohnstrukturerhebung zulässig sei.
Das Datenschutzgesetz verlangt für die Erhebung von personenbezogenen Daten gesetzliche Grundlagen. Die Lohnstrukturerhebung stützt sich auf Rechtsgrundlagen im Bundesstatistikgesetz und in der Statistikerhebungsverordnung des Bundesrates ab. Art. 5 Bundesstatistikgesetz überträgt die Kompetenz für die Anordnung obligatorischer Erhebungen von Personendaten dem Bundesrat. Dieser hat die Lohnstrukturerhebung einschliesslich der Erhebung der AHV-Versichertennummer im Anhang zur Statistikerhebungsverordnung angeordnet.

Der Umgang mit Informationen im Rahmen statistischer Tätigkeiten des Bundes untersteht klaren Regeln. Insbesondere darf Erhebungsmaterial, das persönliche Identifikationsnummern enthält, nur von zuständigen Erhebungsstellen bearbeitet werden und ist zu vernichten, sobald die Auswertung abgeschlossen ist. Die Ergebnisse dürfen nur so veröffentlicht oder zugänglich gemacht werden, dass die befragten Personen, Haushalte oder Unternehmen nicht identifiziert werden können. Die Datenschutzstelle konnte HRZ wegen der klaren rechtlichen Ausgangslage grünes Licht für die Bekanntgabe der Lohnstrukturerhebungsdaten inklusive AHV-Versichertennummer geben.

[15] Art. 50e AHVG, SR 831.10.

PID-Nummer auf Stimmrechtsausweisen

Mit der Einführung des Registerharmonisierungsgesetzes des Bundes (RHG) wurde die Führung der kommunalen Einwohnerregister in der ganzen Schweiz weitgehend vereinheitlicht. Im RHG wird insbesondere definiert, welche persönlichen Merkmale der Einwohnerinnen und Einwohner in den Registern mindestens erfasst werden müssen. Zu diesen Informationen gehört neben Angaben, die seit jeher in den Einwohnerregistern geführt werden – Name, Vorname, Adresse, Geburtsdatum, Zuzug und Wegzug – die AHV-Versichertennummer. Parallel zur AHV-Versichertennummer vergibt und führt das Personenmeldeamt der Stadt Zürich für alle Einwohnerinnen und Einwohner eine eigene, stadtinterne Nummer, die PID-Nummer (Personen-Identifikations-Nummer).

Die PID-Nummer wird unter anderem auf den städtischen Stimmrechtsausweisen verwendet, wo sie bis anhin im Adressfeld abgedruckt wurde. Daran störte sich eine Privatperson und bat die Datenschutzstelle um Auskunft, ob eine solche Verwendung zulässig sei. Um diese Frage zu beantworten, musste zuerst geprüft werden, ob die Führung einer internen PID-Nummer parallel zur AHV-Versichertennummer überhaupt zulässig ist.

Das Registerharmonisierungsgesetz verlangt, das Stimm- und Wahlrecht im Einwohnerregister zu erfassen, in welchem auch die AHV-Versichertennummer erfasst wird. Zur Erleichterung von Geschäftsprozessen kann das Einwohnerregister auch eine interne PID-Nummer verwenden. Die Verwendung einer solchen internen, bloss sektoriellen PID-Nummer kann nicht nur zulässig, sondern mit Blick auf künftige Entwicklungen – beispielsweise im Bereich E-Government – sogar angezeigt sein. Sie kann die Gefahr unzulässiger Verknüpfungen von Personendatensammlungen mit anderen Registern (über die AHV Versichertennummer) minimieren.

Auch darf die PID-Nummer auf Stimmrechtsausweisen verwendet werden. Bisher war die PID-Nummer sichtbar im Adressfeld platziert. Die Datenschutzstelle hat dem Bevölkerungsamt empfohlen, die PID-Nummer auf dem Stimmrechtsausweis so zu platzieren, dass diese nicht mehr auf dem Kuvert sichtbar ist. Das Personenmeldeamt ist dieser Empfehlung nachgekommen.

8 Anspruch auf Berichtigung falscher Informationen

Die Verwaltung hat dafür zu sorgen, dass sie keine falschen Informationen bearbeitet. Geschieht dies dennoch, kann verlangt werden, dass unrichtige Personendaten berichtigt werden. Doch wie verhält es sich, wenn Informationen nicht ohne Weiteres als richtig oder falsch bezeichnet werden können?

Im Allgemeinen

Das Datenschutzrecht gewährt Personen, die von einer behördlichen Datenbearbeitung betroffen sind, verschiedene Rechtsansprüche. Damit diese Rechte überhaupt in Anspruch genommen werden (können), muss es für eine betroffene Person zunächst einmal möglich sein, zu erfahren, ob und welche Daten über sie bearbeitet werden. Gegenüber der Zürcherischen Verwaltung ist dieser Anspruch auf Zugang zu eigenen Personendaten aufgrund von § 20 Abs. 2 IDG gegeben. Da dieses Auskunftsrecht quasi am Anfang der Rechtsansprüche steht, wird es als das bedeutendste Institut der Datenschutzgesetzgebung bezeichnet. Über das Auskunftsrecht hinaus stehen betroffenen Personen weitere Rechte zu, so insbesondere ein Berichtigungs- oder Vernichtungsrecht (§ 21 lit. a IDG). Auf Gesetzesstufe (IDG) können diese Rechte immer nur in allgemeiner und abstrakter Weise formuliert sein und müssen in der Praxis entsprechend den Anforderungen und Gegebenheiten der diversen Verwaltungsbereiche umgesetzt und angewendet werden. Dass dies mitunter zu Schwierigkeiten und Klärungsbedarf führen kann, zeigte sich im Berichtsjahr vor allem im Polizeibereich.

POLIS-Datenbank der Polizei

Die Ombudsfrau ersuchte die Datenschutzstelle, ausgehend von Anfragen und Gesuchen, die bei ihr eingegangen waren, um Beurteilung der Frage, ob und in welchem Umfang eine betroffene Person eine Richtigstellung bzw. Gegendarstellung von Einträgen in der polizeilichen Datenbank POLIS verlangen könne. Im Fokus der Abklärungen standen dabei Daten, die nicht ohne Weiteres als richtig oder unrichtig beurteilt werden können. Bei vielen Personendaten ergibt sich deren Richtigkeit bzw. Unrichtigkeit nicht in einer abstrakten oder absoluten Weise, so vor allem bei subjektiven Werturteilen, persönlichen Ansichten oder Schlussfolgerungen.

Die Datenschutzstelle kam zum Ergebnis, dass das Berichtigungsrecht gemäss § 21 IDG, auf welches die POLIS-Verordnung ausdrücklich verweist, auch das Recht beinhaltet, zu Datenbearbeitungen Stellung zu nehmen, welche einer Beurteilung als richtig oder unrichtig nur schwer zugänglich sind. Wie dieses Recht im Einzelnen bezeichnet und ausgestaltet wird (Berichtigungs- oder Bestreitungsrecht, Bestreitungsvermerk, Gegendarstellung oder dgl.), hängt von den jeweiligen Umständen bzw. der konkret zur Diskussion stehenden Datenbearbeitung ab. Die Handhabung der Stadtpolizei, wonach in der polizeilichen Datenbank POLIS in kategorischer Weise nur Berichtigungen zugelassen werden, welche mit Urteil oder amtlichem Schreiben nachgewiesen sind und wonach keine Möglichkeit eines Vermerks bzw. einer Stellungnahme zu polizeilichen Berichten bzw. Rapporten zugelassen wird, widerspricht nach Ansicht der Datenschutzstelle dem Willen des Gesetzgebers, der Lehre und der Rechtsprechung.

Gestützt auf die eingehende Prüfung durch Ombuds- und Datenschutzstelle konnte mit dem Rechtsdienst der Stadtpolizei erreicht werden, dass die Stadtpolizei künftige Gesuche um Berichtigung differenzierter behandeln und auch beantragte Ergänzungen oder Gegendarstellungen entsprechend prüfen wird.

Für weitergehende Informationen zu Sachverhalt, getroffenen Abklärungen, daraus resultierenden Ergebnissen sowie diesbezüglich noch bestehenden Pendenzen wird auf die detaillierte Berichterstattung der Ombudsfrau der Stadt Zürich verwiesen (Bericht 2012, Ziff. 6. Grundsatzfrage: Recht auf Ergänzung und Berichtigung in der POLIS-Datenbank; S. 44 ff.).

9 Auskunft über Erben verstorbener Schuldner

Wenn jemand erbt und die Erbschaft annimmt, erbt er auch offene Schulden des Erblassers. Wie kann ein Gläubiger herausfinden, wer erbt und damit sein neuer Schuldner wird?

Mit dem Tod eines Erblassers geht eine Erbschaft von Gesetzes wegen an die Erben über. Dies betrifft nicht nur das Vermögen des Erblassers, sondern auch dessen Schulden, welche zu persönlichen Schulden der Erben werden[16]. Doch wie kann ein Gläubiger herausfinden, wer die neuen Schuldner sind, wenn sein bisheriger Schuldner verstorben ist? Die Datenschutzstelle klärte dies auf Anfrage des Personenmeldeamtes der Stadt Zürich ab und kam zum Schluss, dass ein Gläubiger die Auskunft, wer Erbe und damit sein neuer Schuldner ist, unter Umständen nur mit Schwierigkeiten oder gar nicht erhält. Und dies obwohl – oder gerade weil – im Kanton Zürich diverse Verwaltungsstellen in den Todesfall eines verstorbenen Schuldners involviert sind.

Das Steueramt der Stadt Zürich verfügt als Inventarisationsbehörde in vielen Erbschaftsfällen über Erbschaftsinformationen. Das Steueramt geht aber grundsätzlich davon aus, dass die Erbfolge in einem Erbfall dem Steuergeheimnis unterliegt, da es sich um nicht allgemein zugängliche Informationen aus dem persönlichen Bereich des Erblassers (beziehungsweise seiner Erben) handelt, die das Steueramt im Zusammenhang mit seiner amtlichen Tätigkeit erhalten hat. Das Steueramt erteilt deshalb aufgrund der steuerrechtlichen Bestimmungen grundsätzlich keine Auskünfte über die Erbfolge an Privatpersonen.

Das Bezirksgericht als Erbschaftsbehörde wird im Kanton Zürich – anders als in anderen Kantonen – in einem Todesfall nicht von sich aus tätig, sondern nur auf Antrag eines Beteiligten (bspw. Testamentseröffnungsverfahren, Ausstellung Erbschein) oder auf Anzeige (bspw. Anordnung sichernder Massnahmen). Die Tatsache, dass eine Schuld des Erblassers noch offen ist, begründet keine Notwendigkeit für sichernde Massnahmen. Ist das Bezirksgericht im Nachlass eines Schuldners bereits aktiv geworden, kann Gläubigern eines Erblassers Auskunft erteilt werden. Wenn aber eine Erbschaftssache beim Bezirksgericht nicht hängig ist, bleibt einem Gläubiger gemäss Auskunft des Bezirksgerichts Zürich nichts anderes übrig, als sich die Information über allfällige Erben anderweitig, in erster Linie wohl beim Zivilstandesamt, zu beschaffen.

Das Zivilstandsamt erteilt aber privaten Gläubigern grundsätzlich keine Auskunft aus den Personenstandsregistern. Gemäss Zivilstandsabteilung des Gemeindeamtes werden einer Privatperson Auskünfte nur erteilt, wenn diese ein besonderes Interesse nachweisen und die Informationen nicht anderweitig beschaffen kann, was schwer zu erfüllen sei.[17] Ausserdem vertritt die Zivilstandsabteilung generell die Meinung, dass die Personenstandsregister nicht wirtschaftlichen Zwecken dienen sollten. Diese restriktive Auskunftspraxis gilt aber nur gegenüber Privaten und tangiert nicht den Informationsaustausch zwischen Zivilstandsämtern, Gerichten und Amtsstellen. Die Zivilstandsämter sind gemäss Zivilstandsverordnung verpflichtet, diesen die zur Erfüllung ihrer gesetzlichen Aufgaben unerlässlichen Personenstandsdaten auf Verlangen bekanntzugeben.

Ein Lichtblick für Gläubiger könnte eine Dienstleistung des Bestattungs- und Friedhofamtes der Stadt Zürich sein[18]. Dieses kennt in Todesfällen Kontaktpersonen und Grabverantwortliche und somit Personen, die oft mit den Erben identisch sein oder letztere mindestens kennen dürften. Das Friedhofamt gibt Dritten zwar keine Auskunft, bietet aber immerhin die Dienstleistung an, Schreiben von Dritten entgegenzunehmen und an die Kontaktpersonen oder Grabverantwortlichen weiter zu leiten.

[16] Art. 560 ZGB.

[17] Art. 59 der Zivilstandsverordnung regelt die Auskunftserteilung an Private wie folgt: «Privaten, die ein unmittelbares und schutzwürdiges Interesse nachweisen, werden Personenstandsdaten bekannt gegeben, wenn die Beschaffung bei den direkt betroffenen Personen nicht möglich oder offensichtlich nicht zumutbar ist.»

[18] Dieses erbringt in der Stadt Zürich die verschiedenen Dienstleistungen rund um die Bestattung eines verstorbenen Menschen.

10 Umgang mit Daten von Verstorbenen

Was passiert mit digitalen Informationen, wenn jemand stirbt? Die Frage stellt sich immer öfter, weil wir uns immer mehr in einer digitalen Welt bewegen. Dies stellt auch die Datenschutzbeauftragten vor neue Probleme. Ein Beispiel aus der Praxis.

Das Leben spielt sich immer mehr in der digitalen Welt ab: Geschäfte werden online abgeschlossen, Korrespondenz wird über E-Mail geführt, soziale Kontakte werden über Netzwerke gepflegt. Da die rasante Entwicklung der Informations- und Kommunikationstechnologie und die wachsende Zahl der Nutzerinnen und Nutzer zu immer umfangreicheren Datenbeschaffungen und -bearbeitungen führen, sind die Datenschutzbeauftragten gefordert. An Veranstaltungen und in Publikationen machen sie regelmässig auf die Gefahren und Risiken für die Persönlichkeitsrechte aufmerksam und empfehlen sowohl Nutzern als auch Anbietern, Massnahmen für einen verbesserten Schutz der Personendaten zu treffen. Wenig Beachtung wurde dabei bisher der digitalen Nachlassplanung geschenkt, obwohl davon auszugehen ist, dass Fragen rund um den Umgang mit Daten von Verstorbenen an Bedeutung gewinnen werden.

Zumindest heute ist davon auszugehen, dass die Mehrheit der Nutzenden zu Lebzeiten keine diesbezüglichen Anordnungen getroffen hat, obwohl verschiedene Möglichkeiten zur digitalen Nachlassplanung bestehen. Aus erbrechtlicher Sicht ist festzuhalten, dass nur urheberrechtlich geschützte Daten von der Universalsukzession erfasst werden, und Persönlichkeitsrechte nicht auf die Erben übergehen.

Dass digitale Informationen eines Verstorbenen auch für seine Hinterbliebenen von grosser Bedeutung sein können, macht der folgende, der Datenschutzstelle zur Beurteilung vorgelegte Fall deutlich: Es ging um die Frage, ob der Lebenspartnerin eines verstorbenen Mitarbeiters Einsicht in dessen private E-Mails gegeben werden dürfe, die sich in dessen geschäftlichem E-Mail-Konto befanden[19]. Die Lebenspartnerin vermutete, dass ihr Partner mit seiner Pensionskasse korrespondiert oder ein entsprechendes Schreiben vorbereitet habe, um diese zu beauftragen, das im Todesfall auszuzahlende Kapital an sie zu überweisen.

Sowohl das eidgenössische[20] als auch das kantonale Datenschutzrecht enthalten Bestimmungen zur Auskunft über Verstorbene. §19 der kantonalen Verordnung über die Information und den Datenschutz (IDV) hält fest:

«Auskunft über Personendaten von verstorbenen Personen wird erteilt, wenn die gesuchstellende Person ein Interesse an der Auskunft nachweist und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen. Nahe Verwandtschaft sowie im Zeitpunkt des Versterbens bestehende Ehe, eingetragene Partnerschaft und eheähnliche Lebensgemeinschaft mit der verstorbenen Person begründen ein Interesse.»

Die Bestimmung wird in der Lehre als gesetzeswidrig kritisiert, da das Schweizer Recht keinen postmortalen Persönlichkeitsschutz kennt: Die (zivilrechtliche) Persönlichkeit einer natürlichen Person endet mit dem Tod, damit gehen auch ihre Rechte aus Persönlichkeits- und Datenschutz unter. Für verstorbene Mitarbeitende, die zu Lebzeiten nicht über ihre privaten E-Mails verfügt haben, beispielsweise durch Löschen der Nachrichten oder schriftliche Anordnung, ist deshalb grundsätzlich kein postmortaler Schutz zu beachten. Unabhängig davon, ob die erwähnte Bestimmung gesetzeswidrig ist oder nicht, zeigt sie einen gangbaren Weg auf: Die gesuchstellende Person muss ein Interesse nachweisen können (sofern ein solches nicht bereits gesetzlich vermutet wird), welches möglichen Interessen anderer Personen gegenüberzustellen ist. Ob der Zugang zu privaten E-Mails eines Verstorbenen gewährt werden kann, ist stets unter Würdigung der konkreten Umstände zu entscheiden. Vermögensrechtliche Interessen dürften dabei einen hohen Stellenwert haben. Vor allem, wenn es sich bei den gesuchstellenden Personen um Erben handelt, was diese nachweisen müssen.

Im vorliegenden Fall hat die zuständige Verwaltungsstelle die Einsichtnahme in die privaten E-Mails ihres verstorbenen Mitarbeiters letztlich verweigert, da die Lebensgefährtin sich nicht als Erbin ausweisen und auch keine Einwilligung der Erbengemeinschaft vorlegen konnte.

[19] Gemäss Internet- und E-Mail-Reglement (AS 236.300) ist die private Nutzung des geschäftlichen Accounts grundsätzlich zulässig. Diese Politik wird auch beim neuen REID-Reglement beibehalten, siehe Seite 7.

[20] Vgl. für die materiell identische Bestimmung auf Bundesebene: Art. 1 Abs. 7 der Bundesverordnung zum Datenschutzgesetz (VDSG).

11 Energieplanung

In den Datenbeständen diverser Dienstabteilungen der Stadt Zürich sind Informationen vorhanden, die für die kommunale Energieplanung wichtig sind. Der Energiebeauftragte der Stadt Zürich muss auf diese Daten zugreifen können.

Die Stadt Zürich hat eine kommunale Energieplanung. Sie ist vom Regierungsrat des Kantons Zürich genehmigt und dient als Grundlage, um die Ziele der kommunalen Energiepolitik zu erreichen und die leitungsgebundene Energieversorgung zu Heiz- und Kühlzwecken zu planen. Die kommunale Energieplanung muss regelmässig aktualisiert und an bauliche Entwicklungen angepasst werden. Um den gesetzlichen Auftrag zu erfüllen, sind Analysen des Gebäudebestands und der Gebäudenutzung notwendig.

Solche Daten sind im Gebäude- und Wohnungsregister (GWR) sowie in verschiedenen Datenbeständen diverser Dienstabteilungen der Stadt Zürich vorhanden. Die bundesrechtlichen Regelungen zum Gebäude- und Wohnungsregister sehen ausdrücklich vor, dass Kantone und Gemeinden Registerdaten in einem bestimmten Umfang für die öffentliche Aufgabenerfüllung nutzen dürfen[21]. Auch gestützt auf kantonales Recht ist die Nutzung der in den Dienstabteilungen vorhandenen Daten für Planungszwecke grundsätzlich möglich[22]. Für allenfalls bei der Stadt Zürich und den Energieversorgern vorhandene energiewirtschaftliche Daten besteht sogar eine Pflicht, diese für die Energieplanung zur Verfügung zu stellen.

Die Datenschutzstelle hat den städtischen Energiebeauftragten auf Anfrage über die Möglichkeiten des Datenzugangs für die Energieplanung beraten und koordinierend unterstützt. Dieser hatte bisher nur einen beschränkten, für einzelne Analysen gültigen Zugang zu Daten aus dem Gebäude- und Wohnungsregister und den Datenbeständen der Dienstabteilungen.

Mit Unterstützung der Datenschutzstelle konnte erreicht werden, dass der Energiebeauftragte in Zukunft regelmässig Daten des Gebäude- und Wohnungsregisters beziehen darf. Die Stadt Zürich konnte hierfür mit dem Bundesamt für Statistik einen entsprechenden Vertrag abschliessen.[23] Auch hinsichtlich der weiteren Informationen aus den Dienstabteilungen, welche für die Energieplanung benötigt werden, konnte veranlasst werden, dass der Energiebeauftragte dazu effizienteren Zugang erhalten wird.

[21] Art. 10 Abs. 3bis Bundesstatistikgesetz, SR 431.01; Verordnung über das Eidgenössische Gebäude- und Wohnungsregister, SR 431.841. [22] § 18 IDG. Für die Energieplanung bestehen gestützt auf § 4 Abs. 2 Energieveordnung, LS 730.11, entsprechende Mitwirkungspflichten. [23] Für das eidgenössische GWR ist das Bundesamt für Statistik verantwortlich. Mit Genehmigung des BFS führt die Stadt Zürich beziehungsweise Statistik Stadt Zürich ein städtisches GWR.

12 Medizinische Gutachten im Stadtarchiv

Im Stadtarchiv lagern Akten der Vormundschaftsbehörden, die medizinische oder psychiatrische Gutachten enthalten können. Ein Forschungsinstitut beantragte Zugang zu diesen Dossiers.

Die Akten der städtischen Vormundschaftsbehörden[24] werden nach Ablauf der gesetzlichen Aufbewahrungsfristen im Archiv der Stadt Zürich archiviert. Solche Akten können von Vormundschaftsbehörden in Auftrag gegebene beziehungsweise in die Akten genommene medizinische oder psychiatrische Gutachten enthalten, beispielsweise bei Fremdplatzierungen von Kindern und Jugendlichen. Ein Forschungsinstitut, das sich mit diesen Gutachten, den Behördenentscheiden und ihren Auswirkungen auf die Betroffenen auseinander setzen wollte, beantragte Zugang zu solchen Vormundschaftsdossiers im Archiv. Auf Anfrage des Stadtarchivs klärte die Datenschutzstelle die Frage, ob medizinische Gutachten nach Übergabe an das Archiv dem ärztlichen Berufsgeheimnis unterstellt sind, und unter welchen Voraussetzungen der Zugang gewährt werden könnte.

Die berufliche Schweigepflicht gemäss Art. 321 StGB sowie das in Art. 321bis StGB geregelte medizinische Forschungsgeheimnis gelten ausschliesslich für die in diesen Bestimmungen erfassten Berufe. Im Bereich der Medizin sind das Ärzte, Zahnärzte und medizinische Hilfspersonen. Weder die Vormundschaftsbehörde noch das Stadtarchiv unterliegen diesen strafrechtlichen Bestimmungen. Deshalb muss keine Bewilligung bei der Eidgenössischen Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung eingeholt werden. Für medizinsche oder psychiatrische Gutachten in Vormundschaftsdossiers sind die Vormundschaftsbehörden und nach Archivierung der Akten das Stadtarchiv verantwortlich. Der Schutz dieser Akten wird durch das allgemeine Amtsgeheimnis sowie das Archiv- und Datenschutzrecht sichergestellt.

Gemäss Art. 10 des Archivgesetzes richtet sich die Einsicht in Archivbestände nach den Bestimmungen des Gesetzes über die Information und den Datenschutz (IDG). Dieses erlaubt die Bekanntgabe von Personendaten, einschliesslich besonders schützenswerten Personendaten, für nicht personenbezogene Zwecke wie Forschung oder Statistik. Voraussetzung ist, dass die Personendaten anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf die Personen möglich sind (§ 18 IDG). In der Praxis führt dies dazu, dass derjenige, der zu Forschungszwecken Zugang zu Personendaten wünscht, ein Gesuch einreichen und darlegen muss, wie die Informationen geschützt, aufbewahrt, anonymisiert und vernichtet werden. Wenn alle Voraussetzungen erfüllt sind, ist die Einsicht in medizinische oder psychiatrische Gutachten im Stadtarchiv für nicht personenbezogene Forschungszwecke grundsätzlich zulässig.

Damit die hohen gesetzlichen Anforderungen im Umgang mit sensiblen Personendaten eingehalten werden können, velangt das Stadtarchiv von Forschenden die Unterzeichnung einer Geheimhaltungserklärung, in welcher sie sich unter anderem zur Einhaltung der folgenden Regeln verpflichten:

- Besondere Personendaten dürfen das Stadtarchiv nicht verlassen.
- Akten dürfen nur im Lesesaal des Stadtarchivs eingesehen werden.
- Akten und Unterlagen dürfen nicht kopiert werden.
- Abschriften müssen vollständig anonymisiert werden.
- Alle Informationen dürfen nur für die bewilligten Zwecke verwendet werden.

Diese Massnahmen sowie die gelegentlichen Rückfragen des Stadtarchivs an die Datenschutzstelle zeigen, dass das Stadtarchiv den Zugang zu sensiblen Daten sorgfältig und zurückhaltend erteilt.

[24] Seit Inkrafttreten des neuen Kindes- und Erwachsenenschutzrechts per 1.1.2013 heisst die Vormundschaftsbehörde Kindes- und Erwachsenenschutzbehörde (KESB).

13 Gesundheitsmonitoring

Der Schulärtzliche Dienst befragte Sekundarschülerinnen und -schüler nach ihrem Lebensstil und ihrem Gesundheitsverhalten. Aus datenschutzrechtlicher Sicht war vor allem die Gewährleistung einer freiwilligen und anonymen Teilnahme ein Anliegen.

Im Schuljahr 2007/08 hat der Schulärztliche Dienst der Stadt Zürich fast alle städtischen Sekundarschülerinnen und -schüler über ihr Gesundheitsverhalten und ihren Lebensstil befragt. Die Umfrageergebnisse stiessen auf grosse Resonanz[25]. Die Datenschutzstelle hatte damals den Schulärztlichen Dienst beratend unterstützt.

Mit dem Ziel, Veränderungen im Gesundheitsverhalten und Lebensstil aufzuzeigen, den Erfolg der Präventions- und Gesundheitsförderprogramme zu prüfen und Hinweise auf neue Trends zu erhalten, wurden im Berichtsjahr erneut rund 2‘000 Sekundarschülerinnen und -schüler befragt. Der Fragebogen, der von Schulärztlichem und Schulpsychologischem Dienst, Suchtpräventionsstelle und Fachstelle für Gewaltprävention ausgearbeitet wurde, enthielt einige hochsensible Fragen. Unter anderem über Medikamentenkonsum, Beeinträchtigung durch gesundheitliche Beschwerden, Alkohol- und Drogenkonsum, Mobbing und den ersten Geschlechtsverkehr. Um die Umfrage auszuwerten, wurde ein externer Partner engagiert. Die neue, am 1. Oktober 2010 in Kraft getretene Datenschutzverordnung der Stadt Zürich (DSV) verlangt, für so sensible Umfragen die Vorabkontrolle durch die Datenschutzstelle.

Im Rahmen dieser Vorabkontrolle hat die Datenschutzstelle vom Schulärztlichen Dienst verlangt, die Befragungs- und Auswertungsprozesse schriftlich zu erläutern bzw. zu dokumentieren sowie den Entwurf des Vertrages mit dem externen Partner vorzulegen. Zentrales Anliegen von Datenschutzstelle und Projektleitung war, dass Freiwilligkeit, Vertraulichkeit und Anonymität der Umfrage jederzeit gewährleistet blieben. Aus diesem Grund wurde der Fragebogen uncodiert und unpersönlich verteilt und die demographischen Angaben wurden so definiert, dass keine Rückschlüsse auf einzelne Schülerinnen oder Schüler möglich waren. Ausserdem wurden die zulässigen Detailauswertungen im Voraus durch den Schulärztlichen Dienst festgelegt und die Auswertungsmodalitäten mit dem externen Partner vertraglich geregelt.

[25] Veröffentlicht auf der Website des Schulärztlichen Dienstes: www.stadt-zuerich.ch/schularzt.

14 Überwachung am Arbeitsplatz

Eine Arbeitgeberin kann ihre Angestellten unter bestimmten Umständen in einem bestimmten Umfang überwachen, wenn das betrieblich notwendig ist. In der Stadt Zürich sind die Richtlinien klar und in mehreren Reglementen festgehalten. Trotzdem tauchen immer wieder Fragen auf.

Die Überwachung am Arbeitsplatz ist regelmässig Anlass für Anfragen und Beschwerden städtischer Mitarbeitenden bei der Datenschutzstelle. Die wichtigsten Spielregeln sind zwar im Arbeits-, Personal- und Datenschutzrecht, im Internet- und E-Mail-Reglement sowie im REID-Reglement (siehe Seite 7) festgehalten, doch lassen sich damit noch lange nicht alle Fragen beantworten. Wann, womit und wie (lange) spezifische Tätigkeiten oder Verhaltensweisen am Arbeitsplatz durch die Arbeitgeberin überwacht werden dürfen, lässt sich oft erst nach teilweise aufwendigen Abklärungen beantworten. Zwei Beispiele aus dem Berichtsjahr.

Ortung von Dienstfahrzeugen
Dank moderner Fahrzeugortungstechnologie kann die Position jedes Dienstfahrzeuges in Echtzeit bestimmt werden. Ausserdem werden gefahrene Strecken, Aufenthaltsorte und Fahrverhalten aufgezeichnet und sind für Auswertungen verfügbar. Für den Arbeitgeber können unterschiedliche Gründe für eine Fahrzeugortung sprechen. So kann es aus betrieblicher Sicht sinnvoll sein zu wissen, welche Dienstfahrzeuge sich in der Nähe eines Stör- oder Notfalls befinden, um einen Mitarbeiter schnell an den Einsatzort zu beordern. Auf der anderen Seite lassen Positionsdaten aber Verwendungsmöglichkeiten zu, die aus Sicht des Mitarbeiters beziehungsweise seines Persönlichkeitsschutzes problematisch sein können. So kann eine Fahrzeugortung je nach Ausgestaltung einer weitgehenden Überwachung am Arbeitsplatz gleichkommen, die unter Umständen übermässig und somit rechtwidrig sein kann (sogenannte Verhaltensüberwachung).

Deshalb stellt sich die Frage, wie sich die unterschiedlichen, aber berechtigten Interessen der Arbeitgeber und der Arbeitnehmer unter einen Hut bringen lassen. Ausgangslage muss die betriebliche Notwendigkeit sein, die einer umfassenden, kritischen und unvoreingenommenen Prüfung standhalten muss. Diesem Aspekt sind die Interessen der Mitarbeitenden gegenüberzustellen. Mit der Erhebung und Auswertung von Informationen soll nur soweit in die Persönlichkeitssphäre der Mitarbeitenden eingegriffen werden, wie es die betriebliche Notwendigkeit erfordert. Anschliessend gilt es, Transparenz und Nachvollziehbarkeit zu schaffen. Einerseits durch klare Regeln für den Umgang mit solchen Informationen, andererseits durch die umfassende Information der Mitarbeitenden. Die Datenschutzstelle stellt immer wieder fest, dass nicht der Einsatz einer Fahrzeugortung oder anderen Technologie zur Arbeitsplatzüberwachung an sich von den Mitarbeitenden als problematisch empfunden wird. Zu Unbehagen am Arbeitsplatz oder Misstrauen gegenüber den Vorgesetzten beziehungsweise der Arbeitgeberin führt meistens die Intransparenz im Umgang mit den Informationen.

Im September 2012 hatte der Stadtrat der Stadtverwaltung den Erlass eines neuen «Reglements über die Benützung und Vermietung von Dienstfahrzeugen»[26] zur Vernehmlassung unterbreitet. Da die Positionsdaten (GPS) für die Mitarbeitenden grossen Zündstoff mit sich bringen und diese Technologie in Zukunft vermehrt in Dienstfahrzeugen eingesetzt werden dürfte, schlug die Datenschutzstelle vor, das Thema Fahrzeugortung im Reglement direkt zu regeln oder im Reglement mindestens eine (ergänzende) Reglementierung durch die zuständige Dienstabteilung zu verlangen. Diesem Vorschlag folgte die Stadtverwaltung: Das am 1.1.2013 in Kraft getretene Reglement sieht vor, dass eine Dienstabteilung, die weitere Daten bearbeiten will als die, die für die Abwicklung von Schadenfällen abschliessend aufgezählt sind, ein separates Reglement erlassen muss[27].

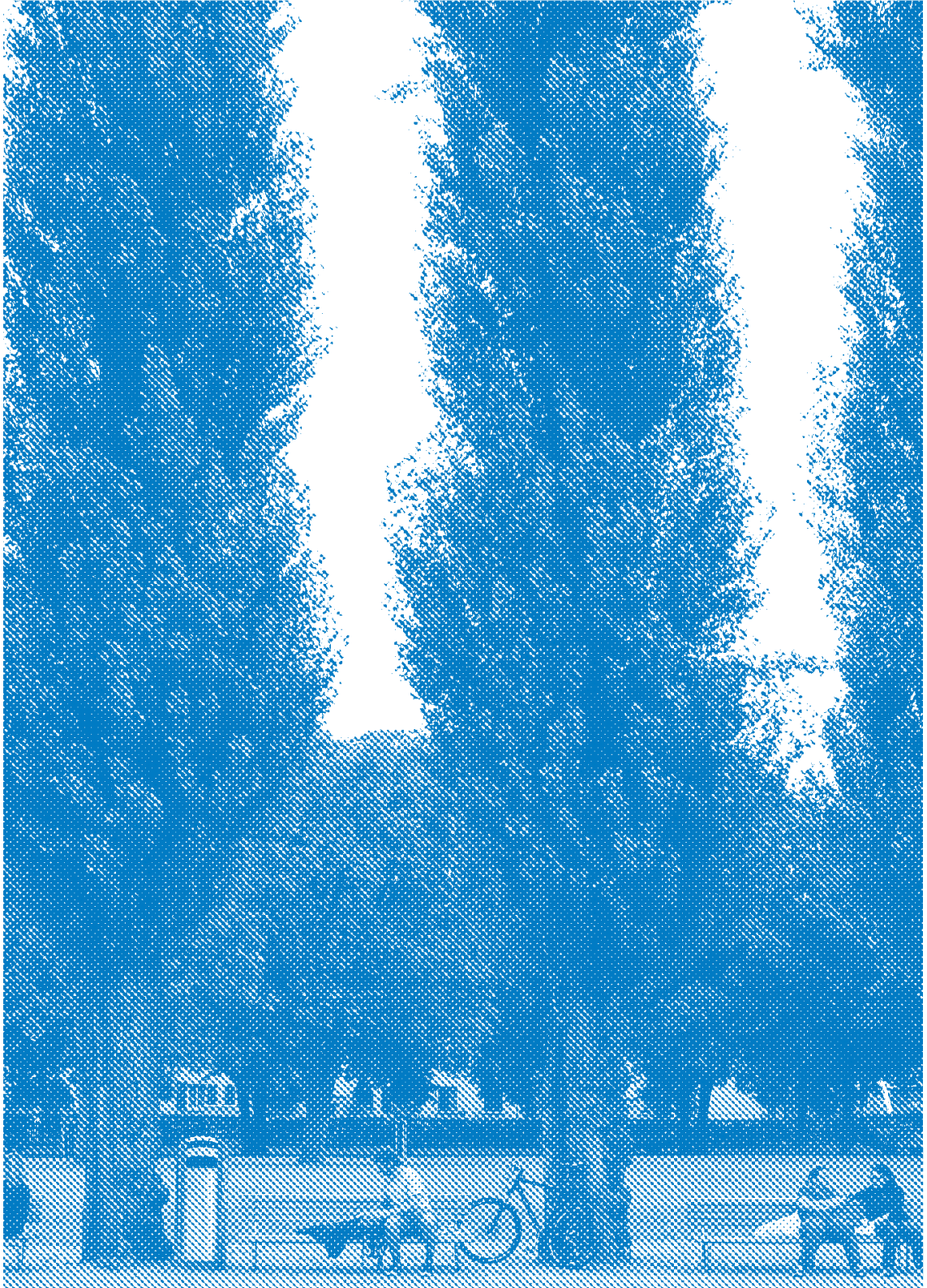
Badgeschliesssystem
Zutrittsberechtigungen werden zunehmend mit elektronischen Badgesystemen geregelt und erteilt. Dadurch werden immer auch Daten über die zutrittsberechtigte Person generiert[28]. Mitarbeitende der VBZ wandten sich an die Datenschutzstelle, nachdem sie über das «Badgeschliesssystem für VBZ eigene WC-Anlagen an den Endhaltestellen» orientiert wurden. In dieser Mitteilung war unter anderem zu lesen:

«Die letzten 1'000 Eintrittsbewegungen werden registriert und bei Bedarf durch die gemäss Datenschutzbestimmungen berechtigten Mitarbeiter ausgelesen.»

Da diese Aussage aus datenschutzrechtlicher Sicht verschiedene Fragen offen liess, bat die Datenschutzstelle den Projektleiter, ihr allfällige Projektunterlagen zum Badgeschliesssystem zu schicken, und einige Fragen zu beantworten. Von Interesse waren vor allem der Zweck der Registrierung und die Auswertungen der Eintrittsbewegungen. Gemäss VBZ ereigneten sich in WC-Anlagen an Endhaltestellen mehrere Vandalenakte. Die Registrierung mit Badge beziehungsweise die Auswertung der Zutrittsdaten sollte helfen, fehlbare Personen identifizieren und für Schäden an den WC-Anlagen zur Verantwortung ziehen zu können.

[26] STRB 1385 vom 31. Oktober 2012. [27] Art. 5 Abs. 3 Reglement über die Benutzung und Vermietung von Dienstfahrzeugen. [28] Vgl. zum elektronischen Badgesysteme auch TB 2010, 20 ff.

Die Datenschutzstelle machte die VBZ darauf aufmerksam, dass Aufzeichnungen der Eintritte nur zulässig sind, wenn sie geeignet und erforderlich sind, um den angestrebten Zweck zu erreichen (Verhältnismässigkeit). Sie wies darauf hin, dass insbesondere das Erfordernis der Geeignetheit nicht gegeben oder zumindest nicht erkennbar und nachvollziehbar sei. Die Datenschutzstelle wies die VBZ wiederholt darauf hin, dass die entscheidende Frage sei, wie einem Einzelnen durch die Auswertung der letzten 1'000 Eintritte ein Vandalenakt nachgewiesen werden soll. Dabei gilt zu berücksichtigen, dass die WC-Anlagen stark frequentiert sind (rund 100 Eintritte täglich) und sich der Tatzeitpunkt nur ungefähr bestimmen lässt. Diese zentrale Frage konnte die VBZ letztlich nicht beantworten und akzeptierte, dass die Auswertung der Zutrittsdaten aus datenschutzrechtlichen Überlegungen nicht zulässig ist. Die Datenschutzstelle forderte die VBZ auf, ihre Mitarbeitenden über die Aufhebung der Datenerhebung und -auswertung zu informieren.



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

Marcel Studer, RA lic. iur.,
Datenschutzbeauftragter (80%)

Yvonne Jöhri, Dr. iur.
juristische Mitarbeiterin (80%)

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

Monika Niederberger
Sekretariat (20%)

Stadt Zürich
Datenschutzbeauftragter
Beckenhofstrasse 59
8006 Zürich

Tel. 044 363 24 42
Fax 044 363 24 43

datenschutz@zuerich.ch
www.stadt-zuerich.ch/datenschutz

Quelle Fotos:
Mediendienste der Stadt Zürich
Zentralkomitee der Zünfte Zürichs

Gestaltung:
SPUTNIK Vertot, Luzern