Stadt Zürich
Datenschutzbeauftragter

Tätigkeitsbericht 2010

Der Datenschutzbeauftragte hat dem Stadtrat und 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 2010 bis 31. Dezember 2010 ab.

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

*Art. 19 ADSV, § 39 IDG

Abkürzungsverzeichnis

ADSV	Allgemeine Datenschutzverordnung der Stadt Zürich vom 5. November 1997 (AS 236.100)
AS	Amtliche Sammlung der Stadt Zürich, www.stadt-zuerich.ch/internet/as/home.html
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); in Kraft seit 1. Oktober 2008
IDV	Verordnung über die Information und den Datenschutz des Kantons Zürich vom 28. Mai 2008 (LS 170.41); in Kraft seit 1. Oktober 2008
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

Inhaltsverzeichnis

Ein Schwerpunkt der Beratungs- und Prüfungstätigkeit der Datenschutzstelle im Berichtsjahr 2010 war die Thematik *Veröffentlichung von Informationen im Internet.* Vor allem mit Verweis auf das im Kanton Zürich geltende Öffentlichkeitsprinzip wird im Rahmen von Projekten zunehmend auch eine Veröffentlichung von Informationen im Internet angestrebt. Im Gegensatz zum Datenschutzgesetz auf Bundesebene fehlen auf kantonaler Ebene spezifische Regelungen, welche die Koordination zwischen Öffentlichkeitsprinzip und Datenschutz betreffen. In der Praxis stellen sich deshalb rechtliche Fragen, deren Beantwortung im Einzelfall regelmässig nicht einfach ist (vgl. die Fälle Nr. 7 – 12). Die Grundsätze, welche die Stadtverwaltung bei Veröffentlichungen von Informationen im Internet zu beachten hat, sind aber immer dieselben – zusammengefasst die folgenden:

Tue Gutes und sprich darüber – und stell's ins Internet?
Sind von der Veröffentlichung im Internet auch Personendaten betroffen, liegt eine Bekanntgabe von Personendaten im Sinne der Datenschutzgesetzgebung vor. Sollen Informationen im Internet veröffentlicht werden, empfiehlt die Datenschutzstelle, das jeweilige Vorhaben unter folgenden Gesichtspunkten zu planen und zu prüfen:

– *Personendaten gehören nicht ins Internet*
Die Veröffentlichung im Internet ist eine Publikationsform, die grosses Potential für Persönlichkeitsverletzungen mit sich bringt. Aufgrund der spezifischen Risiken von Internetpublikationen kann grundsätzlich jede Bekanntgabe von Personendaten schützenswerte private Interessen (in irreversibler Weise) gefährden. Bei der Veröffentlichung von Personendaten im Internet ist daher grundsätzlich Zurückhaltung geboten.

– *Keine Regel ohne Ausnahme: aber nur mit Rechtfertigungsgrund*
Wie jede andere Bekanntgabe von Personendaten muss sich auch eine Publikation im Internet entweder auf eine ermächtigende Rechtsgrundlage oder auf die Einwilligung der Betroffenen abstützen können. Die Rechtsgrundlagen finden sich in den Spezialgesetzgebungen wie bspw. im Geoinformationsgesetz des Bundes. Je sensibler die Personendaten, die im Internet publiziert werden sollen, zu beurteilen sind, umso klarer muss sich aus der gesetzlichen Grundlage eine entsprechende Ermächtigung ergeben. Analoges gilt in Bezug auf Einwilligungserklärungen.

– Das Öffentlichkeitsprinzip macht nicht alles öffentlich

Die Verwaltung ist zu einer aktiven Informationstätigkeit von Amtes wegen verpflichtet: § 14 IDG verlangt, dass die Verwaltung über Tätigkeiten von allgemeinem Interesse informiert. Diese Verpflichtung kann aber nicht als Ermächtigung für beliebige Internetpublikationen verstanden werden, denn die Bekanntgabe von Personendaten ist nur in Ausnahmefällen von allgemeinem Interesse. Dies kann bspw. bei Personen des öffentlichen Lebens oder bei Personen, die in besonderer Beziehung zur Verwaltung (Vertragspartner) stehen, gegeben sein. Eine weitere Ausnahme gilt bspw. für Verwaltungsangestellte, wenn und soweit sie öffentliche Aufgaben erfüllen, so dass in amtlichen Dokumenten deren Namen und Funktionsbezeichnungen angegeben werden dürfen. Abgesehen von derartigen Ausnahmefällen lässt sich aber eine Veröffentlichung von Personendaten nicht mit dem Öffentlichkeitsprinzip rechtfertigen.

– Wenn immer möglich anonymisieren

Das Fehlen einer Ermächtigung zur Veröffentlichung von Personendaten bedeutet nicht zwingend, dass die Verwaltung auf eine Internetpublikation verzichten muss. Informationen können in der Regel so aufbereitet werden, dass diese keine personenbezogenen Angaben beinhalten und keine Rückschlüsse auf bestimmte Personen ermöglichen. Mit der Anonymisierung von Informationen kann erreicht werden, dass eine Publikation – aus datenschutzrechtlicher Optik – zulässig ist.

– Es muss nicht immer Internet sein

§ 14 IDG (Informationstätigkeit von Amtes wegen) äussert sich nicht zur Wahl des Kommunikationsmittels. Weder verpflichtet noch rechtfertigt § 14 IDG pauschal Veröffentlichungen über Internet. Bei der Wahl des Kommunikationsmittels sind vielmehr die allgemeinen Grundsätze des IDG zu beachten: im Umgang mit Personendaten ist dies namentlich der Grundsatz der Verhältnismässigkeit. Eine Informationstätigkeit über Internet lässt sich nur rechtfertigen, falls sich der Zweck der Veröffentlichung nicht durch ein anderes – weniger weitgehendes und die Persönlichkeit der Betroffenen in geringerem Masse tangierendes – Kommunikationsmittel erreichen lässt.

– In jedem Falle: die Interessenabwägung

Die Interessenabwägung nach § 23 IDG ist bei jeder Bekanntgabe von Information – ob im Internet oder anderswo – vorzunehmen. Alle möglichen öffentlichen und privaten Interessen, die für oder gegen eine Internetpublikation sprechen, sind zu eruieren und einer entsprechenden Wertung zu unterziehen. Diese (umfassenden) Interessensabwägungen sind oft nicht einfach, aber nichts desto trotz unerlässlich.

– Frühzeitige Beratung

Aufgrund der mit Internetpublikationen einhergehenden «besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen» (§ 10 IDG), wird empfohlen, Projekte mit personenbezogenen Veröffentlichungen im Internet der Datenschutzstelle frühzeitig zu melden, damit diese die Projektleitung beraten und die Notwendigkeit einer (formellen) Vorabkontrolle prüfen kann.

[1] GR-Nr. 2010/139.

[2] TB 2009, S. 5 ff.

[3] AS 551.190; Über Entstehung und Inhalt dieser Verordnung hat die Datenschutzstelle regelmässig berichtet (TB 2009 S. 9; TB 2008 S. 9; TB 2007 S. 10; TB 2006 S. 11).

[4] Grund der Befristung war in erster Linie die unsichere Rechtsentwicklung auf Bundesebene zum Zeitpunkt der Entstehung der städtischen Verordnung (2007 – 2009). Der Grund für die kurze Frist von bloss einem Jahr ist demgegenüber auf «Verzögerungen» im städtischen Gesetzgebungsprozess zurückzuführen (Rückweisung an Stadtrat, Behördenreferendum; vgl. TB 2008 S. 9).

[5] GR-Nr. 2010/418.

1 Neuerlass Städtische Datenschutzverordnung (DSV)

Im letztjährigen Tätigkeitsbericht hat die Datenschutzstelle die Weisung des Stadtrats für den Neuerlass einer städtischen Datenschutzverordnung (DSV) vom 24. März 2010[1] vorgestellt.[2] Im Berichtsjahr war der Datenschutzbeauftragte an mehrere Sitzungen der vorberatenden Kommission (GPK) eingeladen und konnte zu den Anträgen der Gemeinderätinnen und Gemeinderäte Einschätzungen und Stellungnahmen abgeben sowie entsprechende Vorschläge einbringen.

Erwartungsgemäss waren die Voraussetzungen für den Einsatz von Videoüberwachung die meist diskutierten und umstrittensten Bestimmungen der Vorlage. Im Rahmen der parlamentarischen Vorberatungen blieb dies die einzige Regelung, welche grundlegend neu formuliert wurde. Die übrigen Bestimmungen wurden von der Kommission – mit Ausnahme einiger wenigen Änderungen bzw. Präzisierungen – akzeptiert. Der Gemeinderat hat die Vorlage am 30. März 2011 beraten und gutgeheissen und in der Schlussabstimmung vom 25. Mai 2011 genehmigt. Die Inkraftsetzung der neuen Städtischen Datenschutzverordnung (DSV) ist Sache des Stadtrats.

2 Polizeiliche Datenbank GAMMA

Die am 1. Januar 2010 in Kraft getretene Verordnung über die polizeiliche Datenbank GAMMA[3] war gemäss Schlussbestimmung bis zum 31. Dezember 2010 anwendbar. Eine derart kurze Befristung der Anwendbarkeit auf bloss ein Jahr darf für eine formellgesetzliche Rechtsgrundlage mit Sicherheit als ungewöhnlich bezeichnet werden.[4] Der Stadtrat beantragte Ende September 2010 beim Gemeinderat eine Verlängerung der Verordnung um 2 Jahre.[5] Im Rahmen dieser Vorlage wurde die Datenschutzstelle um Stellungnahme zur geplanten Verlängerung der Verordnung über die polizeiliche Datenbank GAMMA angefragt. Der Datenschutzbeauftragte äusserte sich in seiner Stellungnahme dahingehend, dass für die Beurteilung der Verlängerung in erster Linie massgebend sei, ob der Zweck der GAMMA-Verordnung – die Früherkennung und Verhinderung von Gefährdungen der öffentlichen Sicherheit und Ordnung anlässlich von Sportveranstaltungen – erreicht werden konnte.

Aufgrund der erst wenige Monate dauernden Aktivzeit von GAMMA konnte Ende September 2010 – für die Datenschutzstelle nachvollziehbar – allerdings noch keine zuverlässige Aussage über Nutzen und Wirksamkeit von GAMMA gemacht werden. Zwar lag bereits der erste der gemäss Verordnung von der Stadtpolizei jährlich vorzulegende Bericht über Nutzen und Wirksamkeit von GAMMA[6] vor, doch umfasste dieser nur die Anfangszeit von Januar bis Mai 2010. Aufgrund dieser Ausgangslage war auch die gewünschte datenschutzrechtliche Beurteilung bzw. Einschätzung nicht möglich.

Da der Gemeinderat über die beantragte Verlängerung nicht vor Ablauf der Frist beschliessen konnte, verfügte der Vorsteher des Polizeidepartements die Sistierung der Datenbank GAMMA ab 1. Januar 2011.

3 Reglement Benutzung elektronische Infrastruktur

Mitte 2009 hat der Stadtrat das «Reglement über die Nutzung und Überwachung von Internet und E-Mail» in Kraft gesetzt.[7] Wie sich bereits aus der Bezeichnung des Reglements ergibt, beschränkt sich dieses auf Internet und E-Mail[8]. Im Rahmen der Ausarbeitung des Reglements war man sich bereits damals bewusst, dass zu einem späteren Zeitpunkt auch die Telefonie in dieses Reglement aufgenommen werden muss, da diese in Zukunft nicht mehr über Telefonleitungen, sondern auch über das Züri-Netz bzw. das Internet abgewickelt werden sollte. Da die konkrete Telefonietechnologie für die Stadtverwaltung zum damaligen Zeitpunkt aber noch zu wenig bekannt war und die Themen Internet und E-Mail dringend geregelt werden mussten, beschränkte man sich zunächst auf die Regelung von Internet und E-Mail.

Inzwischen ist die Internettelefonie in der Stadtverwaltung weitgehend Realität geworden. Aus diesem Grund prüfte der Datenschutzbeauftragte das Bestehen eines allfälligen Handlungs- und Regelungsbedarfs im Bereich der Telefonie und stellte fest, dass es an klaren und verbindlichen Spielregeln und vor allem auch an Transparenz für die Nutzung weitgehend fehlt. Entsprechende Anfragen von Mitarbeitenden der Stadtverwaltung bei der Datenschutzstelle zur neuen Internettelefonie, insbesondere zur Aufzeichnung und Löschung von Telefongesprächen, bestätigten diese Feststellungen. Das Manko besteht vor allem darin, dass die Mitarbeitenden nicht informiert sind bzw. nicht wissen, welche Informationen bei wem, zu welchem Zweck und

[6] Art. 13 Abs. 2: «Die Stadtpolizei kontrolliert die Einhaltung dieser Vorschriften. Sie erstattet dem Polizeidepartement, der Geschäftsprüfungskommission des Gemeinderates und der oder dem Datenschutz beauftragten der Stadt jährlich Bericht über die technischen und organisatorischen Massnahmen zur Gewährleistung dieser Vorschriften. Der Bericht enthält auch statistische Auswertungen sowie Angaben zu Nutzen und Wirksamkeit von GAMMA.»

[7] Über Entstehung und Inhalt hat die Datenschutzstelle regelmässig berichtet, vgl. TB 2007, S. 7; TB 2008, S. 8; TB 2009, S. 8.

[8] Im Einzelnen informiert dieses die Mitarbeiterinnen und Benutzerinnen der städtischen Infrastruktur darüber, wie sie Internet und E-Mail nutzen dürfen und wann und von wem ihr Tun allenfalls kontrolliert bzw. überwacht werden kann.

in welcher Weise bearbeitet werden, ob und wie die Telefonie-Infrastruktur der Stadtverwaltung zu privaten Zwecken genutzt werden darf und welche Kontroll- oder Überwachungsmöglichkeiten bestehen und eingesetzt werden.

Der Datenschutzbeauftragte initialisierte aus diesem Grund anfangs 2010 die Einsetzung einer Arbeitsgruppe, welche seither an der Ausarbeitung eines neuen Reglements arbeitet[9]. Allerdings wurde – sowohl angesichts des städtischen Projekts VoIP (Voice over IP/Telefonie über Internet) als auch im Hinblick auf die allgemein zu erwartende elektronische Entwicklung – bald klar, dass nur eine allgemeine Regelung Sinn macht und eine Beschränkung auf einzelne Dienste bzw. eine (zusätzliche) Reglementierung der Telefonie zu eng wäre. Die Arbeitsgruppe hat sich denn auch zum Ziel gesetzt, ein allgemeines Reglement der Benutzung der elektronischen Infrastruktur der Stadt Zürich zu erarbeiten, welches auch dem Multimedia-Ansatz (Bereitstellung verschiedener Dienste wie bspw. Telefonie, Internet, E-Mail über eine Infrastruktur, unabhängig vom – insbesondere auch mobilen – Endgerät) Rechnung trägt.

4 Prostitutionsgewerbeverordnung

In der Stadt Zürich wird seit einiger Zeit an einer Vorlage für eine Verordnung über das Prostitutionsgewerbe gearbeitet. Da Informationsbearbeitungen im Kontext von Prostitution auch von datenschutzrechtlicher Relevanz sind, wurde die städtische Datenschutzstelle um Mitarbeit in einer der Arbeitsgruppen angefragt

Mitte Januar 2011 hat der Stadtrat den Entwurf einer Prostitutionsgewerbeverordnung nun diversen Verwaltungsstellen und privaten Institutionen zur Vernehmlassung unterbreitet. Wie sich der Vernehmlassungsvorlage des Polizeidepartements entnehmen lässt, wurde auf eine allgemeine Melde- und Registrierungspflicht für alle sich prostituierenden Personen (entgegen dem Ansinnen der Stadtpolizei) verzichtet. Zu Beginn der Arbeiten stand eine solche umfassende Meldepflicht noch zur Diskussion und Prüfung. Aus datenschutzrechtlicher Sicht hätte ein derartiges Vorhaben allerdings kaum gerechtfertigt werden können, da flächendeckende Meldepflichten regelmässig weit über das Ziel hinausschiessen und damit unverhältnismässig

9 Die neue Arbeitsgruppe setzt sich – wie bereits jene, welche unter der Leitung des Datenschutzbeauftragten das «Reglement über die Nutzung und Überwachung von Internet und E-Mail» erarbeitet hat – ebenfalls wieder aus Vertreterinnen und Vertretern aus dem Departementssekretariat des Finanzdepartements, HR Stadt Zürich (HRZ) und Organisation und Informatik der Stadt Zürich (OIZ) zusammen.

sind. Die Datenschutzstelle begrüsst denn auch den Verzicht auf eine allgemeine Melde- und Registrierungspflicht für alle sich prostituierenden Personen im Entwurf der Prostitutionsgewerbeverordnung.

In ihrer Stellungnahme von Ende März 2011 richtete die Datenschutzstelle ihr hauptsächliches Augenmerk auf die Frage, wie klar und erkennbar aus der neuen Prostitutionsgewerbeverordnung hervorgeht, welche Daten durch die Polizei erhoben und zu welchen Zwecken diese weiterbearbeitet werden.[10] Unter diesem Gesichtspunkt beurteilte sie die im Entwurf der Prostitutionsgewerbeverordnung vorgesehenen Datenbearbeitungen v.a. hinsichtlich der Bewilligungspflicht für Salonbetreiber als zu offen formuliert. Nach Auffassung der Datenschutzstelle ist aus dem Verordnungsentwurf in Anbetracht der Sensibilität der Informationen nicht mit genügender Bestimmtheit erkennbar, für welche Zwecke Personendaten bearbeitet werden (dürfen). Dies hat auch zur Folge, dass sich weder bestimmen lässt, welche Daten benötigt werden, noch beurteilt werden kann, ob die Daten verhältnismässig erhoben und weiterbearbeitet werden. Damit erfüllt der Verordnungsentwurf die gesetzliche Anforderung der genügenden Bestimmtheit gemäss § 8 Abs. 2 IDG nicht.

5 Staatsschutz

Im Sommer 2010 stand der Staatsschutz erneut im Zentrum des öffentlichen Interessens und die Medien proklamierten einen «neuen Fichenskandal».[11] Auslöser dieser breit geführten Debatte war in erster Linie ein Bericht der Geschäftsprüfungsdelegation des Bundes, welcher diverse Mängel im Bereich des Staatsschutzes aufzeigte.[12] Auch die Schweizerischen Datenschutzbeauftragten beschäftigten sich bereits seit einiger Zeit mit dem Thema Staatsschutz.[13] In ihrer Medienmitteilung vom September 2010 haben sie darauf hingewiesen, dass die Unabhängigkeit der Datenschutzaufsicht im Staatsschutz nicht gewährleistet sei und dass es an einer wirksamen Kontrolle über die Staatsschutztätigkeit von Bund, Kantonen und Gemeinden gleich in mehrfacher Hinsicht fehle, und zwar in Form einer parlamentarischen Kontrolle durch die Geschäftsprüfungsorgane der Legislativen (Oberaufsicht), einer Kontrolle durch die vorgesetzten Stellen (Dienstaufsicht) sowie einer Kontrolle durch die unabhängigen Datenschutzstellen (Datenschutzaufsicht).[14]

[10] § 8 Abs. 2 IDG verlangt, dass das Bearbeiten besonderer Personendaten einer hinreichend bestimmten Regelung in einem formellen Gesetz bedarf (Personendaten im Kontext von Prostitution sind als besondere Personendaten im Sinne von § 3 IDG zu qualifizieren). Das Erfordernis der formellgesetzlichen Grundlage wird mit einer Verordnung, welche durch den Gemeinderat beschlossen wird, erfüllt.

[11] So bspw. die Berichterstattung im Tages-Anzeiger vom 1. Juli 2010.

[12] Bericht vom 21. Juni 2010, abrufbar unter www.admin.ch.

[13] Der Datenschutzbeauftragte der Stadt Zürich ist Mitglied einer Arbeitsgruppe der Schweizerischen Datenschutzbeauftragten (privatim), welche sich im Berichtsjahr eingehend mit dem Thema Staatsschutz beschäftigt hat. Im Berichtsjahr hat der Datenschutzbeauftragte die städtische Geschäftsprüfungskommission (GPK) mehrmals über die rechtliche Situation der Staatsschutztätigkeit in der Stadt Zürich informiert.

[14] Medienmitteilung vom 2. September 2010 der Schweizerischen Datenschutzbeauftragten (privatim), abrufbar unter www.privatim.ch.

[15] Art. 35 und 35a V-NDB; SR 121.1.

[16] § 14 Polizeiorganisationsgesetz (POG); LS 551.1.

[17] Art. 6 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS); SR 120.

[18] Vgl. www.uvek.admin.ch.

[19] PBG; SR 745.1.

[20] EBG; SR 742.101.

[21] Verordnung über die Videoüberwachung im öffentlichen Verkehr; SR 742.147.2. Diese Verordnung findet auf den konzessionierten Bereich der VBZ direkt Anwendung. Die bisherige Verordnung über die Videoüberwachung im öffentlichen Verkehr des Kantons Zürich wird durch die neue Bundesverordnung abgelöst.

[22] Art. 54 Abs. 1 PBG bestimmt, dass Unternehmen für ihre konzessionierten und bewilligten Tätigkeiten, d.h. für die regelmässige und gewerbsmässige Personenbeförderung, den Art. 16 – 25 bis DSG unterstehen. Die Aufsicht richtet sich gemäss Art. 54 Abs. 3 PBG nach Art. 27 DSG, wonach der EDÖB zuständig ist.

[23] In der Lehre wurde dies als verfassungswidrig kritisiert, so bspw. Rudin Beat, Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, in SJZ 2009, 1 ff.

Seit Oktober 2010 verlangt die bundesrätliche «Verordnung über den Nachrichtendienst des Bundes», dass die (kommunale) Staatsschutztätigkeit durch eine (kommunale) Dienstaufsicht überprüft wird.[15] Im Übrigen überlässt die erwähnte Verordnung die konkrete Organisation der Dienstaufsicht den kantonalen und kommunalen Vollzugsorganen. Da in der Stadt Zürich die sicherheitspolizeilichen Aufgaben in erster Linie der Stadtpolizei (und nicht der Kantonspolizei) obliegen[16], gilt die Stadt Zürich – gleich wie die Kantone – als Vollzugsorgan im Bereich des Staatsschutzes[17]. Die vom Bundesrecht verlangte Dienstaufsicht existiert für die Stadt Zürich noch nicht. Das Polizeidepartement der Stadt Zürich hat der Datenschutzstelle gegenüber aber zugesichert, dass die Regelung der Dienstaufsicht über die Stadtpolizei im Bereich der Staatsschutztätigkeit mit hoher Priorität an die Hand genommen werde. Sobald feststeht, wie die verwaltungsinterne Dienstaufsicht aussieht und was sie beinhaltet, werden die Geschäftsprüfungskommission und die Datenschutzstelle prüfen, welche Kontrollpflichten und -kompetenzen verwaltungsexternen Aufsichtsstellen (Oberaufsicht durch die GPK; Aufsicht durch die Datenschutzstelle) zustehen müssen.

6 Bahnreform 2

Per 1. Januar 2010 sind auf Bundesebene im Rahmen der sog. Bahnreform 2[18] das neue Personenbeförderungsgesetz[19] sowie das revidierte Eisenbahngesetz[20] in Kraft getreten. Diese Bundeserlasse wirken sich in datenschutzrechtlichen Belangen unmittelbar auf die VBZ und die Zuständigkeit der Datenschutzstelle aus.

Mit der Bahnreform 2 wurde u.a. das Ziel verfolgt, dass für alle Transportunternehmen im konzessionierten und bewilligten Tätigkeitsbereich die gleichen Bestimmungen bezüglich Datenbearbeitung und Datenschutz Anwendung finden sollen. Neu gelten deshalb bspw. für die Videoüberwachungen in den Trams und Bussen der VBZ die Bestimmungen des Bundesrechts.[21] Aber auch hinsichtlich der datenschutzrechtlichen Aufsicht und Kontrolle ist mit Inkrafttreten der beiden erwähnten Bundeserlasse eine wesentliche Änderung eingetreten: Die datenschutzrechtliche Aufsicht über die VBZ im Bereich der konzessionierten und bewilligten Tätigkeiten steht neu dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu. Kraft Bundesrecht[22] untersteht damit – zum ersten Mal – eine städtische Verwaltungsstelle der datenschutzrechtlichen Aufsicht des Bundes.[23]

Aufgrund der Gesetzesrevisionen auf Bundesebene hatte die VBZ zu klären, welche Tätigkeitsbereiche als konzessioniert[24] zu qualifizieren sind und in den Zuständigkeitsbereich des EDÖB fallen und welche Bereiche nach wie vor (als nicht konzessionierte Bereiche) unter der Aufsicht der städtischen Datenschutzstelle stehen. Es zeigte sich, dass sich diese Abgrenzung trotz bzw. wegen der Bahnreform 2 nicht mit der gewünschten Klarheit aus den rechtlichen Grundlagen ableiten lässt. In Zusammenarbeit zwischen VBZ und städtischer Datenschutzstelle wurde präzisiert, welcher Datenschutzstelle (Bund oder Stadt) die datenschutzrechtliche Aufsicht über die wichtigsten Datenbearbeitungen zusteht. Demnach stehen in Zukunft insbesondere folgende Datenbearbeitungen der VBZ unter der Aufsicht des EDÖB: Fahrgastzählungen, Kundendatenbank, Datenpool Schwarzfahrer, Marketing-Cross-Selling, Videoüberwachung und ZVV-Projekte in Zusammenhang mit der Bearbeitung von Kundendaten. Für die übrigen Datenbearbeitungen der VBZ gilt nach wie vor das kantonale und kommunale Datenschutzrecht und somit die Zuständigkeit der städtischen Datenschutzstelle. Dies betrifft insbesondere: Datenschutzfragen im Personalbereich oder in Zusammenhang mit Verträgen und Rechtsmittel, welche nicht die beförderten Fahrgäste betreffen.

Mit der zwischen VBZ und städtischer Datenschutzstelle getroffenen Regelung hat sich der EDÖB einverstanden erklärt. Die VBZ, die Datenschutzstelle der Stadt Zürich wie auch der EDÖB sind sich einig, dass für diese Abgrenzungsfrage keine abschliessende Regelung getroffen werden kann und dass auch in Zukunft Datenbearbeitungen zur Diskussion stehen können, bei welchen im Bedarfsfalle die Frage nach der Aufsichtszuständigkeit situativ durch die Beteiligten geklärt werden muss.

7 Veröffentlichung von georeferenzierten Informationen

Bei raumbezogenen Informationen besteht oft Unklarheit und Rechtsunsicherheit darüber, ob diese als Personendaten im Sinne der Datenschutzgesetzgebung zu gelten haben, da sich ein Personenbezug via Georeferenzierung bspw. nur über das Grundbuch herstellen lässt[25]. Die Abgrenzung von Sachdaten und Personendaten ist aufgrund der zunehmenden Verfügbarkeit und Möglichkeiten zur Verknüpfung von Geodaten mit Personendaten immer schwieriger. Aus diesem Grund wird der Umgang mit solchen Daten zunehmend in spezialgesetzlichen Erlassen geregelt: So wird auf

[24] Die Konzession nach EBG umfasst den Bahnbetrieb inkl. Einrichtung und Unterhalt von Anlagen sowie Führung der Stromversorgungs-, Betriebsleit- und Sicherheitssysteme.

[25] Die Rechtspraxis geht davon aus, dass Geodaten dann Personendaten i.S. der Datenschutzgesetzgebung darstellen, wenn eine Verknüpfung mit einer Person besteht oder mit vernünftigem Aufwand hergestellt werden kann (BBl 2006 7851 f.).

[26] Bundesgesetz über Geoinformationen (Geoinformationsgesetz, GeoIG, SR 510.62) mit zugehöriger Geoinformationsverordnung (GeoIV, SR 510.620).

[27] Und zwar derart, dass jene Daten, welche im Internet öffentlich zugänglich zu machen sind, in Gesetz und Verordnung ausdrücklich aufgeführt werden.

[28] Antrag des Regierungsrates vom 8. Juni 2010; abrufbar unter www.kantonsrat.zh.ch.

[29] So der Tatbestand gemäss § 10 IDG, welcher eine Vorabkontrolle bei der Datenschutzstelle erforderlich macht.

[30] Im Vergleich zu anderen Formen der Datenbekanntgabe ist die Veröffentlichung im Internet diejenige Publikationsform, die das grösste Potential für Persönlichkeitsverletzungen mit sich bringt; vgl. dazu einleitend S. 2 ff.

[31] Im Einzelnen geht es um folgende Daten: Bau- und Zonenordnung, Denkmalpflegeinventar, Inventar der schützenswerten Gärten und Anlagen von kommunaler Bedeutung, Inventar der kommunalen Natur- und Landschaftsschutzgebiete, Daten der amtlichen Vermessung (Grundstücke), Verkehrsbaulinien, Waldgrenzen, Parkplatzverordnung und Quartierplanverfahren.

Bundesebene seit dem 1. Juli 2008 der Umgang mit Geoinformationen des Bundesrechts geregelt[26]. Gegenstand ist dabei auch die Veröffentlichung von Geoinformationen im Internet[27]. Auf kantonaler Ebene existiert zur Zeit noch keine entsprechende Regelung für kantonale und kommunale Geoinformationen; immerhin liegt aber bereits eine bereinigte Gesetzesvorlage für ein Kantonales Geoinformationsgesetz (KGeoIG) vor, welche im Juni 2010 vom Regierungsrat zuhanden des Kantonsrats verabschiedet wurde[28].

Im Berichtsjahr wurden der Datenschutzstelle zwei Projekte gemeldet, bei welchen es um die Veröffentlichung von georeferenzierten Informationen im Internet geht. Aufgrund der mit Internetpublikationen oft einhergehenden «besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen»[29], dürfte es geboten sein, Projekte mit personenbezogenen Veröffentlichungen im Internet der Datenschutzstelle regelmässig zu melden, damit diese die Notwendigkeit einer Vorabkontrolle prüfen kann[30]. Die Datenschutzstelle beurteilte die beiden Projekte, bei denen die Gefahr von Persönlichkeitsverletzungen aufgrund der veröffentlichten Informationen als gering einzuschätzen ist, wie folgt:

Projekt Katasterauskunft

Im Rahmen des Projekts Katasterauskunft sollen verschiedene städtische Inventare und Kataster im Internet publiziert werden und zwar derart, dass über jedes Grundstück auf Stadtgebiet Informationen zu Einzelthemen oder ein Gesamtbericht zur Parzelle abgerufen werden können[31].

Die Datenschutzstelle wies darauf hin, dass die Frage, ob für alle der geplanten Internet-Veröffentlichungen genügende Rechtsgrundlagen vorhanden seien, aufgrund der heutigen Rechtslage kontrovers beantwortet werden könne. Sobald jedoch der Entwurf des Kantonalen Geoinformationsgesetzes – der in weiten Teilen der Regelung von Geoinformationen des Bundesrechts entspricht – in der vorliegenden oder in vergleichbarer Form in Kraft treten wird, werden die gesetzlichen Grundlagen für die geplanten Veröffentlichungen im Internet klar gegeben sein.

Aufgrund dieser Ausgangslage sowie in Anbetracht dessen, dass von der geplanten Veröffentlichung nur Informationen betroffen sind, welche nicht

als sensibel zu qualifizieren sind, hielt es der Datenschutzbeauftragte für vertretbar, die geplanten Katasterauskünfte im Internet zugänglich zu machen. Verantwortlich für die Veröffentlichungen aus den verschiedenen Fachbereichen ist und bleibt aber letztlich die jeweils zuständige Stelle bzw. Dienstabteilung[32], welcher somit auch die Prüfung der Rechtsgrundlage für jede Internet-Veröffentlichung in ihrem Fachbereich sowie der Entscheid über Umfang und Art der Veröffentlichung obliegt.

Im Januar 2011 wurde die Katasterauskunft online geschaltet und die Öffentlichkeit über das neue Angebot informiert[33].

Projekt Solardachkataster

Mit dem geplanten Solardachkataster[34] (Projekt mapSolar) soll im Hinblick auf die Erreichung der Ziele der 2000-Watt-Gesellschaft auf die umweltschonende Solarenergie hingewiesen werden. Dazu soll das Solarstrom- und Solarwärmepotential für jedes Gebäudedach in der Stadt Zürich über eine Web-Applikation im Internet veröffentlicht werden. Die gewählte Darstellung soll – durch die Kategorisierung und Zuordnung jedes Dachs zu einer der farblich unterschiedlich gekennzeichneten Kategorien – nicht nur einen Überblick darüber geben, wie geeignet ein Dach zur solarthermischen oder photovoltaischen Nutzung ist, sondern auch erlauben, mit einem Klick auf ein Dach die entsprechenden Detailinformationen abzurufen.

Die Datenschutzstelle wies u.a. darauf hin, dass die geplante Internet-Veröffentlichung personenbezogene Informationen beinhalte und sich deshalb auf eine ermächtigende Rechtsgrundlage stützen lassen muss[35]: Weder die Umweltschutzgesetzgebung, noch Art. 2ter der Gemeindeordnung[36], noch die Geoinformationsgesetzgebung enthält eine Ermächtigung für die geplanten Veröffentlichungen. § 9 E-KGeoIG sieht allerdings vor, dass für die Geobasisdaten des kommunalen Rechts und die andern Geodaten der Gemeinde der Gemeinderat die entsprechenden Festlegungen treffen kann[37].

Nachdem die Veröffentlichung im Internet – auch nach Prüfung verschiedener Alternativen – nach Angaben von UGZ der einzig gangbare Weg bleibt, soll eine entsprechende Rechtsgrundlage auf kommunaler Ebene geschaffen werden. Zur Zeit wird eine entsprechende Rechtsgrundlage erarbeitet.

32 Grün Stadt Zürich, Amt für Städtebau, Tiefbauamt.

33 Abrufbar unter www.kastasterauskunft.stadt-zuerich.ch.

34 Dieses wurde vom GIS-Kompetenzzentrum im Auftrag von Umwelt- und Gesundheitsschutz Zürich (UGZ) erarbeitet.

35 Vorliegend wurde insbesondere die Verhältnismässigkeit der personenbezogenen Veröffentlichung im Internet in Frage gestellt, da für die Information der Öffentlichkeit anonymisierte bzw. statistische Zahlen ausreichen würden (bspw. wieviel % der Dächer der Stadt Zürich könnten mit Solaranlagen ausgestattet werden und wieviel % Energie könnte dadurch eingespart werden).

36 Art. 2ter der Gemeindeordnung der Stadt Zürich verpflichtet die Gemeinde, sich aktiv für den Schutz und die Erhaltung der natürlichen Lebensgrundlagen und für einen schonenden Umgang mit den natürlichen Ressourcen einzusetzen sowie zur Umsetzung einer nachhaltigen Entwicklung, LS 101.100.

37 Darunter ist die Exekutive, d.h. der Stadtrat, zu verstehen (siehe Weisung des Regierungsrates vom 8. Juni 2010 zu § 9, S. 22).

[38] § 16 Abs. 1 IDG.

[39] § 14 IDG.

[40] Die Veröffentlichung von Personendaten (im Internet) dürfte sich ohnehin nur in speziellen Fällen auf § 14 IDG stützen lassen, da ein allgemeines Interesse an einer solchen (aktiven) Veröffentlichung von Personendaten durch die Verwaltung i.d.R. fehlen dürfte. Siehe dazu einleitend S. 2 ff.

8 Veröffentlichung von Personendaten in Verzeichnissen

Statistik Stadt Zürich publizierte seit über 40 Jahren quartalsweise ein sog. «Verzeichnis der Bautätigkeit». Nebst zahlreichen statistischen Informationen zur Bautätigkeit in der Stadt Zürich wurden für jedes Bauvorhaben – aufgelistet nach Quartieren – auch Angaben zu Bauherrschaft und Projektverfasser bekannt gegeben. Diese Verzeichnisse waren im Internet als Download oder auf Anfrage hin in gedruckter Version frei erhältlich. Gegen diese Veröffentlichungspraxis beschwerte sich ein Bauherr bei der städtischen Datenschutzstelle. Er machte geltend, dass bei Eingabe seines Namens in einer Internet-Suchmaschine persönliche Angaben allgemein zugänglich würden, für deren Veröffentlichung weder eine ermächtigende Rechtsgrundlage noch ein öffentliches Interesse vorhanden seien.

Nach Angaben von Statistik Stadt Zürich führte die bisherige namentliche Bekanntgabe von Bauherrschaft und Projektverfasser noch nie zu Reklamationen oder Beanstandungen. Aus diesem Grunde sowie unter Berücksichtigung der Tatsache, dass in den erwähnten Verzeichnissen nur diejenigen personenbezogenen Angaben wiedergegeben werden, die bereits im Baubewilligungsverfahren veröffentlicht wurden, sei die Publikation der Verzeichnisse der Bautätigkeit stets als korrekt angesehen worden. So verständlich diese Einschätzung auch sein mag, die eingehende Prüfung der Angelegenheit, welche die Datenschutzstelle in Zusammenarbeit mit Vertretern des Präsidial- und Hochbaudepartements vorgenommen hat, kommt zu einem anderen Ergebnis. Ausgangspunkt bildet die gesetzliche Anforderung, dass sich die Bekanntgabe von Personendaten – auch wenn es sich wie vorliegend nicht um sensible Daten handelt – auf eine ermächtigende Rechtsgrundlage abstützen lassen muss.[38] Eine solche Rechtsgrundlage existiert für die erwähnten Verzeichnisse nicht und auch die amtliche Informationspflicht, welche Teil des Öffentlichkeitsprinzips darstellt, kann vorliegend nicht als Rechtsgrundlage herangezogen werden. Eine Informationspflicht (und somit auch ein Informationsrecht) besteht nur in Bezug auf Tätigkeiten der Verwaltung, die von allgemeinem Interesse sind[39]. Für die bisherige namentliche Bekanntgabe von Bauherrschaft und Projektverfasser besteht jedoch – im Gegensatz zu den zahlreichen statistischen Informationen – kein öffentliches Interesse[40].

Auch der Umstand, dass die personenbezogenen Angaben im Rahmen der Baubewilligungsverfahren bereits veröffentlicht wurden, vermag die bisherige Veröffentlichungspraxis nicht zu rechtfertigen. Veröffentlichungen von Personendaten durch die Verwaltung führen nicht dazu, dass die publizierten Informationen für weitere Verwendungen quasi frei verfügbar oder zugänglich wären. Amtliche Veröffentlichungen erfolgen stets zu einem konkreten Zweck, welcher sich aus den jeweiligen Spezialgrundlagen ergeben muss (so beginnt bspw. mit der öffentlichen Bekanntgabe der Bauvorhaben die Frist zur Wahrung von Ansprüchen[41]). Auch nach einer Veröffentlichung bleibt die Bearbeitung der Personendaten durch die Verwaltung zweckgebunden, d.h. jede weitere Verwendung muss entweder mit dem ursprünglichen Zweck vereinbar sein oder sich auf andere Rechtsgrundlagen abstützen können.

Gestützt auf diese Beurteilung hat sich Statistik Stadt Zürich entschieden, auf eine weitere Publikation des Verzeichnisses der Bautätigkeit zu verzichten.

9 Veröffentlichung von Einbürgerungsdaten

Einbürgerungsdaten auf dem Webserver des Gemeinderats

Bis Februar 2008 wurde das Bürgerrecht der Stadt Zürich an Ausländer, die nicht in der Schweiz geboren wurden, durch den Gemeinderat erteilt.[42] Gleich wie heute bestand bereits für die damaligen Einbürgerungen durch den Gemeinderat die gesetzliche Pflicht, bestimmte Informationen der Einbürgerungsgesuche im städtischen Amtsblatt zu publizieren.[43] Das städtische Amtsblatt erscheint in gedruckter und elektronischer Form, wobei bei der elektronischen Veröffentlichung seit 2009 der Zugang zu amtlich publizierten Personendaten nach drei Monaten gesperrt werden muss.[44]

Die damaligen Einbürgerungen durch den Gemeinderat wurden allerdings nicht nur im städtischen Amtsblatt publiziert, sondern waren – wie alle Beschlüsse des Gemeinderats – Bestandteil der Gemeinderatsprotokolle und wurden als solche auch auf dem Webserver der Stadt Zürich im Internet allgemein zugänglich gemacht. Die Veröffentlichung der Gemeinderatsbeschlüsse und damit der Gemeinderatsprotokolle stützt sich auf verschiedene Normen des kantonalen und kommunalen Rechts.[45] Eine spezifische Rechtsgrundlage betreffend Veröffentlichung der Gemeinderatsprotokolle im Internet besteht nicht.

41 § 314 ff. PBG (LS 700.1).

42 Seither ist für die Aufnahme von Personen in das Bürgerrecht der Stadt Zürich ausschliesslich der Stadtrat zuständig.

43 §§ 11 und 17 Bürgerrechtsverordnung des Kantons Zürich (LS 141.11); Art. 6 Richtlinie für die Aufnahme von im Ausland geborenen Ausländern in das Bürgerrecht der Stadt Zürich (AS 141.110).

44 Art. 3 Abs. 3 Publikationsverordnung der Stadt Zürich (AS 170.520).

45 §§ 68a und 106 Gemeindegesetz des Kantons Zürich (LS 131.1); Art. 31 Abs. 3 Gemeindeordnung der Stadt Zürich (AS 101.100); Art. 49 Geschäftsordnung des Gemeinderates (AS 171.100); Art. 4 Verordnung über die Parlamentsdienste (AS 171.400).

Bei der Datenschutzstelle haben sich mehrere eingebürgerte Personen über die Publikation der erwähnten Einbürgerungsbeschlüsse des Gemeinderats auf dem Webserver der Stadt Zürich beschwert und die Löschung dieser Informationen verlangt. Es wurde geltend gemacht, dass bei Eingabe ihres Namens in Internet-Suchmaschinen persönliche Angaben[46] über sie abgerufen werden können. Dies störe sie und habe auch schon zu negativen Konsequenzen (Beschimpfung) geführt. Ausserdem sei die Notwendigkeit dieser Publikationen nicht nachvollziehbar, da ihre Einbürgerungsverfahren mehrere Jahre zurücklägen.

Die Datenschutzstelle erachtet die zeitlich unbefristete Internetpublikation von Einbürgerungsdaten in Gemeinderatsprotokollen als unzulässig. Nach der Rechtsprechung des Bundesgerichts stellen Einbürgerungsentscheide Verwaltungsakte und keine politischen Entscheide dar[47] und haben somit insbesondere auch das verwaltungs- und datenschutzrechtliche Verhältnismässigkeitsprinzip zu beachten. Dieses verpflichtet die zuständige Verwaltungsstelle u.a., die unterschiedlichen Interessen, die für oder gegen die Publikation von Einbürgerungsdaten sprechen können, festzustellen und gegeneinander abzuwägen. Einbürgerungsentscheide werden publiziert, um die Öffentlichkeit aktuell über erfolgte Einbürgerungen zu informieren. Gründe, weshalb Einbürgerungsdaten der Öffentlichkeit während mehrerer Jahre zur Verfügung stehen sollen, sind nach Ansicht der Datenschutzstelle nicht ersichtlich. Das Informationsinteresse der Öffentlichkeit über erfolgte Einbürgerungen nimmt mit der Zeit stetig ab und im gleichen Masse nimmt das Interesse der eingebürgerten Personen am Schutz ihrer Privatsphäre je länger je mehr zu. Betrachtet man die vorliegende Problematik schliesslich im Lichte der geltenden Publikationsverordnung, wonach die elektronische Veröffentlichung von Personendaten im Amtsblatt grundsätzlich auf drei Monaten befristet ist, spricht dies ebenfalls dafür, dass Einbürgerungsdaten nach Ablauf einer gewissen Zeit[48] vom Internet zu entfernen sind.

Das Büro des Gemeinderates konnte sich dieser Auffassung der Datenschutzstelle anschliessen und liess sämtliche Einbürgerungsbeschlüsse vom Webserver der Stadt Zürich entfernen.

[46] Publiziert wurden Höhe der Einbürgerungsgebühr, Name, Vorname, Staatsangehörigkeit, Geburtsdatum und -ort, Zivilstand, Vorname und Geburtsdatum der Kinder.

[47] BGE 129 I 232, E. 3.3 S. 237 ff.; 134 I 56, E. 2 S. 58.

[48] Auf die Festlegung einer bestimmten Frist konnte verzichtet werden. Die Einbürgerungsentscheide, die bis Februar 2008 Bestandteil der Gemeinderatsprotokolle waren, sind nicht mehr öffentlich zugänglich und seit März 2008 werden die Einbürgerungsentscheide sowieso nur noch im städtischen Amtsblatt veröffentlicht.

Tagblatt-Publikation der nicht ins Bürgerrecht aufgenommenen Personen

Im Zuge der vorstehend erwähnten Abklärungen hat die Datenschutzstelle festgestellt, dass im Tagblatt der Stadt Zürich nicht nur die Entscheide über die erteilten Bürgerrechte, sondern auch diejenigen über die abgelehnten Gesuche publiziert werden. Nach Ansicht der Datenschutzstelle bestehen jedoch für die Veröffentlichung der abgelehnten Gesuche[49] keine Rechtsgrundlagen, was der Bürgerrechtsabteilung der Stadtkanzlei entsprechend mitgeteilt wurde. Diese hat die Angelegenheit umgehend geprüft und der Datenschutzstelle gegenüber bestätigt, dass in Zukunft abgelehnte Gesuche nicht mehr veröffentlicht werden.

10 Veröffentlichung von Personendaten in Broschüren

Wie heikel die Veröffentlichung von Personendaten – sei es von Mitarbeitenden, sei es von Dritten – sein kann, zeigte ein weiterer Fall aus dem Berichtsjahr: Dabei ging es um die Veröffentlichung von Fotos im Rahmen einer Broschüre der Stadt Zürich, welche in gedruckter Version versandt sowie zusätzlich dazu im Internet in elektronischer Form zum Herunterladen bereit gestellt wurde. In dieser Broschüre waren Personen auf den Fotos gut erkennbar abgebildet. Eine der betroffenen Personen wandte sich daraufhin an die Datenschutzstelle und machte geltend, dass die Fotos ohne ihre Einwilligung gemacht und für die Broschüre verwendet worden seien. Da die Publikation der Fotos in dieser Broschüre für sie stigmatisierend sei, was sich auch anhand von Reaktionen von Arbeitskollegen gezeigt habe, verlangte sie u.a. den Rückruf und die Vernichtung der Broschüre[50].

Die Abklärungen der Datenschutzstelle zeigten schon bald, dass die Parteien die näheren Umstände der Fotoaufnahmen, die über ein Jahr zurücklagen, völlig unterschiedlich in Erinnerung hatten. Unklar bzw. unbeantwortet blieb insbesondere die Frage, ob die betroffene Person über das Fotografieren in ihrem Arbeitsumfeld aufmerksam gemacht worden war und ob sie nicht zwangsläufig aufgrund der Umstände (Profi-Fotograf und offensichtliches Fotoequipment) erkennen musste, dass sie fotografiert wurde. Strittig blieb im Weiteren auch, ob die abgebildeten Personen über den Verwendungszweck der Fotografien, konkret die Veröffentlichung in einer thematisch heiklen Broschüre, orientiert worden sind. Unbestritten war zumindest,

[49] Die nicht in das Bürgerrecht aufgenommenen Personen wurden ebenfalls namentlich und unter Angabe von Staatsangehörigkeit und Wohnadresse publiziert.

[50] Der Forderung, die Broschüre vom Internet zu nehmen, konnte im Sinne einer Sofortmassnahme entsprochen werden.

51 Dabei handelt es sich um ca. 2'100 Personen.

dass die abgebildete Person nie eine schriftliche Einwilligung erteilt hatte und auch unmittelbar vor Drucklegung der Broschüre weder mündlich noch schriftlich um ihr Einverständnis angegangen wurde.

In der schwierigen Auseinandersetzung zwischen den Parteien nahm die Datenschutzstelle in erster Linie eine Art Vermittlerrolle ein. Der Fall, der schliesslich in einem aussergerichtlichen Vergleich beigelegt werden konnte, zeigt exemplarisch das «Minenfeld» bei Veröffentlichungen von Personendaten auf und machte einmal mehr deutlich, dass im Umgang mit Personendaten grösste Sorgfalt angebracht ist. Die Datenschutzstelle empfiehlt deshalb, im Einzelfall jeweils frühzeitig zu klären, wozu und in welcher Form die Einwilligung von betroffenen Personen eingeholt werden muss.

11 Veröffentlichung von Personaldaten im Intranet

Die Stadtpolizei Zürich unterhält im Intranet eine interne Informationsplattform, auf welcher seit ihrer Inbetriebnahme neben «Geschäftsdaten» (Geschäftsadresse, dienstlichen Telefonnummern, UserID für den EDV-Zugriff, Personalnummer, Grad und Funktion) auch verschiedene «Persönliche Daten» (wie Foto, Privatadresse, Geburtsdatum oder (optional) private Telefonnummern oder Zivilstand) aller Angehörigen der Stadtpolizei[51] abgerufen werden konnten. Zugang zu diesen Personalinformationen haben sämtliche Mitarbeitende der Stadtpolizei Zürich, welche Zugang zu einem EDV-Arbeitsplatz haben.

Mitarbeitende der Stadtpolizei, die sich an dieser ihrer Ansicht nach zu weit gehenden Veröffentlichungspraxis von Personaldaten im Intranet störten, gelangten an die Datenschutzstelle mit der Bitte um Prüfung und Beurteilung der Rechtskonformität. Auf schriftliche Anfrage hin bestätigte die Stadtpolizei die geschilderte Praxis und begründete diese in erster Linie mit den Eigenheiten des Polizeibetriebs. So mache es u.a. der 24-Stunden- und der Schicht-Betrieb erforderlich, dass Mitarbeitende, insbesondere in aktuellen und medienträchtigen Fällen, auch in der Freizeit kontaktiert werden könnten. Die Stadtpolizei wies zudem darauf hin, dass seit 2007 zumindest neu eintretende Mitarbeiterinnen und Mitarbeiter mit dem «Revers für Angehörige der Stadtpolizei Zürich» zur Kenntnis nehmen, «dass personenspezifische Daten (Namen/Vornamen/Funktion/Foto) im Intranet bzw. Internet für dienstliche Zwecke veröffentlicht werden können».

Die Datenschutzstelle legte der Stadtpolizei im Folgenden dar, dass die praktizierte Veröffentlichung von privaten Personaldaten sowohl gegen das städtische Personalrecht[52] als auch den datenschutzrechtlichen Grundsatz der Verhältnismässigkeit verstosse[53] und die Erarbeitung einer gesetzeskonformen Lösung aufgrund der geltenden personal- und datenschutzrechtlichen Bestimmungen unumgänglich sei. In der Folge nahm die Stadtpolizei entsprechende Anpassungen an die Hand und orientierte die Datenschutzstelle schliesslich im März 2010 darüber, dass die allgemeinen Leserechte nun auf reine Geschäftsdaten eingeschränkt worden und weitere Personendaten nur noch einem stark eingeschränkten Personenkreis (Vorgesetzte, Mitarbeitende der Einsatzzentrale) zugänglich seien. Die Datenschutzstelle wurde schliesslich auch von Seiten der Mitarbeitenden der Stadtpolizei dahingehend orientiert, dass ihren Anliegen mit der neuen Lösung bzw. mit der Entfernung der persönlichen Daten vom Intranet in genügender Weise Rechnung getragen werde.

12 Veröffentlichung von Videofilmen (sog. Videostreaming)

In der Stadtverwaltung besteht das Bedürfnis, zunehmend auch Videofilme (bspw. von speziellen Sportevents oder Kulturanlässen) auf der städtischen Website zu veröffentlichen (sog. Videostreaming). Da die städtische Infrastruktur nicht auf Videostreaming ausgelegt ist und die hierfür erforderliche Erweiterung sehr kostenintensiv wäre, sucht die Stadtverwaltung nach Alternativen. Als Möglichkeit wird die Publikation der Videos auf externen Plattformen wie YouTube, Twitter oder der eines Schweizer Vertragspartners in Betracht gezogen. Die Internetdienste der Stadtkanzlei und die OIZ haben die Datenschutzstelle gebeten, die Zulässigkeit von Veröffentlichungen von Videofilmen auf externen Plattformen zu beurteilen bzw. sich zu den diesbezüglichen Rahmenbedingungen zu äussern.

Für Veröffentlichungen von Videofilmen stehen aus datenschutzrechtlicher Optik zwei Themen im Vordergrund: Einerseits das (rechtliche) Thema der Zulässigkeit von Veröffentlichungen im Internet an sich, andererseits das (technische) Thema der Datenherrschaft. Hinsichtlich der Anforderungen an die Zulässigkeit ist eine Veröffentlichung von Videofilmen im Internet grundsätzlich gleich wie jede andere Datenbekanntgabe auf einer Website zu beurteilen: Entweder existiert eine gesetzliche Grundlage, die zu einer Publikation von Videofilmen ermächtigt[54], oder es liegen die Einwilligungen

[52] Namentlich Art. 43 PR, welcher die Bekanntgabe von Personendaten abschliessend regelt, insbesondere auch die Veröffentlichung im Intranet (Bst. c). Es liegt auch keine Einwilligung (Bst. b) vor, da die im Revers statuierte Kenntnisnahme von Veröffentlichungen im Intranet bzw. Internet die Anforderungen an eine Einwilligung aus mehreren Gründen nicht zu erfüllen vermag.

[53] Auch unter Berücksichtigung, dass das Bedürfnis an der Zugänglichkeit zu privaten Daten von Mitarbeitenden bei der Polizeiarbeit aufgrund unregelmässiger Arbeitszeiten und Schichtbetrieb höher ist als bei «gewöhnlichen» Arbeitsverhältnissen, ist nicht nachvollziehbar, dass bei der Stadtpolizei rund 2'000 Mitarbeitende für die Erfüllung ihrer Aufgaben jederzeit Zugriff auf die vorhandenen privaten (!) Informationen aller Kolleginnen und Kollegen haben müssen.

[54] Bspw. ermächtigen Art. 74 und 211 der Schweizerischen Strafprozessordnung (StPO), Videobilder zwecks Aufklärung oder Fahndung ins Internet zu stellen.

55 Vgl. zu dieser Thematik bzw. Problematik vorstehend den Bericht Nr. 10 (Veröffentlichung von Personendaten in Broschüren).

56 So kann nicht verhindert werden, dass die veröffentlichten Inhalte kopiert und weiterverbreitet werden oder auch dann noch in einem Internetarchiv öffentlich zugänglich sind, wenn die Inhalte auf der Website bzw. der Publikationsplattform bereits gelöscht worden sind.

57 So hat die in der StPO vorgesehene Internet-Fahndung stets unter Wahrung des Verhältnismässigkeitsgrundsatzes, der Unschuldsvermutung und der Persönlichkeitsrechte der Betroffenen zu geschehen. D.h. es muss ein dringender Tatverdacht bzgl. eines schwerwiegenden Delikts gegeben und andere Fahndungsmassnahmen müssen erfolglos geblieben sein.

58 Wie das Bundesverwaltungsgericht im Urteil vom 27. Mai 2009 (A-3144/2008, Erw. 2.2.4) festgehalten hat, gelten IP-Adressen als personenbezogene Informationen im Sinne der Datenschutzgesetzgebung.

59 Die Google Analytics-Software legt einen sog. First Party Cookie auf dem Rechner der Nutzenden mit einer eindeutigen Identifikationsnummer ab, wodurch Zugriffe auf eine Website einzelnen Nutzenden (bzw. IP-Adressen) zugeordnet werden können.

60 Die Firma Google ist dem Swiss Safe Harbor Vertrag beigetreten, weshalb eine firmeninterne Datenübermittlung in die USA grundsätzlich möglich wäre.

61 § 9 IDG.

62 § 6 IDG; § 25 Abs. 1 IDV.

der auf dem Videomaterial erkennbaren Personen vor. Da die Verwaltung für die Erfüllung ihrer gesetzlichen Aufgaben grundsätzlich nicht auf die Veröffentlichung von Videofilmen im Internet angewiesen ist, fehlt in den gesetzlichen Grundlagen in aller Regel eine entsprechende Ermächtigung. In diesen Fällen sind Videopublikationen deshalb nur mit Einwilligung der auf dem Videomaterial erkennbaren Personen rechtmässig.[55] In technischer Hinsicht ist v.a. zu beachten, dass bei Videostreaming – wie generell bei Veröffentlichungen im Internet – die Herrschaft über das veröffentlichte Filmmaterial faktisch aufgegeben wird.[56] Die faktische Aufgabe der Datenherrschaft im Internet stellt für die Rechte der betroffenen Personen ein erhöhtes Risiko dar, und zwar unabhängig davon, ob Videofilme auf der städtischen oder einer fremden Infrastruktur veröffentlicht werden. Dieser Tatsache ist in gebührendem Masse Rechnung zu tragen, sei es von der Stadtverwaltung mit Blick auf die Anforderungen, welche an Einwilligungserklärungen zu stellen sind, sei es vom Gesetzgeber im Hinblick auf die Schaffung entsprechender Rechtsgrundlagen.[57]

13 Städtische Webstatistik

Im Berichtsjahr haben die Internetdienste der Stadtkanzlei die Datenschutzstelle um eine grundsätzliche Beurteilung gebeten, ob das kostenlose Programm «Google Analytics» für die städtische Webstatistik eingesetzt werden darf. «Google Analytics» ermöglicht die Erstellung von Statistiken über das Nutzungsverhalten von Besucherinnen und Besuchern einer Website. Der Einsatz des Programms setzt voraus, dass die IP-Adresse[58] sowie weitere identifizierende Informationen der Nutzenden[59] an einen Server der Firma Google in die USA übermittelt und dort gespeichert werden[60].

Eine Auswertung von (personenbezogenen) Nutzerdaten durch die Stadtverwaltung zur Erstellung von Webstatistiken ist grundsätzlich zulässig, sofern die Informationen zu keinen anderen Zwecken verwendet, sobald wie möglich anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind[61]. Die Stadtverwaltung kann die Erstellung von Webstatistiken auch an eine externe Drittperson übertragen; ein solcher Auftrag hat dann aber zwingend schriftlich und mit dem gesetzlich verlangten Mindestinhalt zu erfolgen[62].

Die Datenschutzstelle hat nach einer ersten (summarischen) Prüfung erhebliche Zweifel, dass ein Einsatz von «Google Analytics» datenschutzkonform ausgestaltet werden kann. Insbesondere lässt sich auf Grund der von der Firma Google festgelegten Nutzungs- und Datenschutzbestimmungen sowie der – weder überschau- noch kontrollierbaren – technischen Ressourcen dieses Unternehmens nicht ausschliessen, dass personenbezogene Daten der Website-Nutzenden nicht auch zu anderen Zwecken (als nur für die Erstellung anonymisierter Webstatistiken) verwendet und bspw. an Partnerunternehmen der Firma Google weitergegeben werden[63]. Damit wäre der Preis für die Kostenlosigkeit des Webstatistik-Tools «Google-Analytics» die Offenlegung persönlicher Informationen der Website-Nutzenden.

14 Elektronische Badgesysteme

Die neuen elektronischen Hausschlüssel dienen heutzutage nicht mehr nur der Türöffnung und Zutrittskontrolle, sondern verfügen aufgrund der integrierten Chiptechnologie zunehmend auch über weitergehende Funktionalitäten. So können elektronische Schlüssel stadtintern bspw. auch als Badge für die Zeiterfassung eingesetzt oder als elektronisches Portemonnaie zum Bezahlen in Personalcafeterias genutzt werden.

Die Datenschutzstelle nahm eine Anfrage betreffend der Nutzung von Schlüsseln als Zahlungsmittel zum Anlass, sich von der IMMO einen Überblick über die mit dem elektronischen Schlüssel verbundenen Systeme zu verschaffen. Aus datenschutzrechtlicher Sicht interessierte dabei insbesondere die Frage, ob mit diesen Systemen eine zentrale oder vernetzte Bearbeitung von Informationen (Generierung, Auswertung, Speicherung etc.) verbunden ist und falls ja, welche.

Die Datenschutzstelle wurde betreffend der Verwendung der Schlüssel im Rahmen der einzelnen Funktionen (Zutrittskontrolle, Zeiterfassung, elektronisches Portemonnaie) dahingehend informiert, dass die verschiedenen Daten immer nur dezentral an den jeweiligen Orten der Datengenerierung (Türschlösser, Zeiterfassungssystem, Kassen) gespeichert werden. Es erfolgt somit keine zentrale Speicherung aller mit einem Schlüssel generierter Informationen[64]. Zugriff auf die dezentral gespeicherten Daten hat zudem jeweils nur der jeweilige Anbieter eines Dienstes. So hat bspw. die IMMO

63 Die OIZ IT-Security stuft diese Gefahr in ihrer gegenüber der Datenschutzstelle abgegeben Beurteilung als gross und eine (technische) Kontrollmöglichkeit der Auftragserfüllung als unrealistisch ein.

64 Eine Ausnahme bildet die Speicherung von Schlüsselangaben beim Gebäudezugang ausserhalb der normalen Öffnungszeiten. Ausserhalb der normalen Öffnungszeit können die Aussentüren nur via Leser (Badge-Zugang) elektronisch geöffnet werden. In diesen Fällen werden die Ausweisnummern der Schlüssel in einer zentralen Datenbank max. 7 Tage gespeichert.

65 Das Journal wird benötigt, um eventuelle Fehlbuchungen zu finden und Buchungen zu stornieren.

bzw. deren Fachstelle Schliesssicherheitstechnik nur Zugriff auf «ihr» Segment, d.h. auf die im Zusammenhang mit der Zutrittskontrolle generierten Schlüsseldaten.

Ist der Schlüssel zusätzlich mit der Funktion eines elektronischen Portemonnaies ausgerüstet, hat der jeweilige Benutzer die Möglichkeit, auf seinen Schlüssel einen bestimmten Geldbetrag als Guthaben zu laden und damit in verschiedenen Personalcafeterias zu bezahlen. Beim Bezahlen erfolgt auf dem Schlüssel eine entsprechende Abbuchung. Schlüsseldaten fallen aber auch in der Kasse an, da alle getippten Transaktionen im elektronischen Journal gespeichert werden[65]. Auf dem Journal der Kassen werden für die Abbuchung folgende Angaben registriert: Produkt, Rechnungsbetrag, Guthaben auf Schlüssel vor und nach Abbuchung, Datum, Zeit, eine (von der Kasse generierte) fortlaufende Nummer sowie die ersten Ziffern der Ausweisnummer des Schlüssels.

Indem die Ausweisnummer auf dem Journal der Kasse nur teilweise gespeichert wird und nur die Betreiberin der Personalcafeterias auf die in den Kassen gespeicherten Informationen zugreifen kann, welche ihrerseits wieder keinen Zugang zu den Schlüsselinformationen bei der IMMO hat, ist keine eindeutige Zuweisung zu einer bestimmten Ausweis-/Schlüsselnummer möglich. Die Betreiberin der Personalcafeterias kann aufgrund der anfallenden Daten somit keine Rückschlüsse auf das Konsumverhalten einzelner Personen schliessen.

Wie erwähnt hat auch die IMMO keinen Zugriff, d.h. sie besitzt keine technischen Einrichtungen, um erfolgte Konsumationen oder andere Angaben auf dem Schlüssel im Zusammenhang mit der Verpflegung auslesen zu können. Somit kann auch die IMMO mittels der Schlüssel keine Verbindung zwischen Geldbezügen oder Konsumverhalten und bestimmten Personen herstellen.

Was die Verwendung und Auswertung der mit dem Einsatz von elektronischen Schlüsseln generierten Daten betrifft, bestehen aus datenschutzrechtlicher Sicht keine Beanstandungen. Allerdings hat die Anfrage gezeigt, dass gerade im Bereich von elektronischen Daten immer wieder Unklarheiten und wenig Transparenz besteht, welche Daten bei wem anfallen und was

mit ihnen gemacht wird. Dabei weckt fehlende Transparenz bei Mitarbeitenden regelmässig die Befürchtung von Überwachungen am Arbeitsplatz. Immerhin verspricht sich die Datenschutzstelle mit der Erarbeitung eines Reglements der Benutzung der elektronischen Infrastruktur[66] auch in diesem Bereich mehr Transparenz.

15 Vom Stromzähler zum Smart Meter

Stromzähler sind heutzutage noch meistens in Kellern installiert und finden – ausser dass sie einmal im Jahr abgelesen werden – kaum Beachtung. Die technologische Entwicklung hat aber auch die Strommessung in Privathaushalten erfasst und Stromzähler werden zunehmend Teil von weit vernetzten Computersystemen. Die sog. «Smart Meter» erlauben es, elektrische Geräte der Privathaushalte von überall aus zu überwachen und zu steuern.

Die neuen, intelligenten Stromzähler zeichnen sich u.a. dadurch aus, dass sie nicht nur den Gesamtverbrauch anzeigen, sondern auch Informationen über den zeitlichen Verlauf der individuellen Stromnutzung liefern[67]. Der Einsatz von Smart Metern soll dadurch zu einem effizienten Umgang mit Strom animieren und zu einem sparsameren Stromverbrauch beitragen. Um zu untersuchen, ob der Stromverbrauch in Haushalten durch den Einsatz von Smart Metern (oder durch andere gezielte Information) gesenkt werden kann, haben sowohl die Elektrizitätswerke des Kantons Zürich (EKZ) als auch das Elektrizitätswerk der Stadt Zürich (EWZ) je ein zeitlich befristetes Projekt gestartet: Während das EKZ im Rahmen eines Pilotprojekts bei 1'000 EKZ Kunden die bestehenden Zähler durch neue Smart Meter ersetzt hat[68], handelt es sich beim Projekt des EWZ um eine breit angelegte wissenschaftliche Feldstudie[69] mit 5'000 freiwilligen Testhaushalten in der Stadt Zürich. Bei den in fünf Gruppen aufgeteilten Testhaushalten werden ein Jahr lang drei verschiedene Instrumente eingesetzt: Während in den Haushalten einer Gruppe – wie im Pilotprojekt EKZ – Smart Meter installiert werden, erhalten die anderen Gruppen andere Informationen zu ihrem Stromverbrauch wie individuelle Beratung zum Stromsparen, regelmässige Rückmeldungen zum eigenen Stromverbrauch oder Angaben zum Stromverbrauch in einem vergleichbaren Haushalt. Die Studie soll die Wirksamkeit und den Einfluss der Visualisierung des Stromverbrauchs durch Smart Meter und Energiean-

66 Siehe dazu S. 6 f.

67 So vermögen Smart Meters dem Verbraucher – zusammen mit entsprechenden Visualisierungsmöglichkeiten – sichtbar und in Echtzeit Informationen über den Stromverbrauch zu liefern. Der Verbraucher ist dadurch in der Lage, jederzeit den momentanen Stromverbrauch zu kontrollieren und zu steuern.

68 Das Pilotprojekt des EKZ ist mit 1000 EKZ Kunden in Dietikon im Mai 2010 gestartet und dauert voraussichtlich bis Mai 2012.

69 Die wissenschaftliche Feldstudie wird in Zusammenarbeit mit dem Bundesamt für Energie und den Universitäten Zürich und Lausanne durchgeführt. Befragungen und Datenerhebungen haben im Januar 2011 begonnen und laufen bis Ende 2012.

zeigegeräte im Vergleich zu anderen Informationsmassnahmen aufzeigen und als Entscheidungsgrundlage für eine allfällige (flächendeckende) Einführung von Smart Metern dienen.

Smart Meter sind aus datenschutzrechtlicher Optik in vielerlei Hinsicht interessant: Es handelt sich um Stromzähler, welche den zeitnahen Stromverbrauch anzeigen, Verbraucherprofile erfassen und die elektronische Fernauslesung ermöglichen. Das Augenmerk der Datenschutzbeauftragten ziehen Smart Meter vor allem auch deshalb auf sich, weil die neue Messtechnik eine Bearbeitung von Personendaten darstellt, welche sogar die Erstellung von Persönlichkeitsprofilen erlaubt.

Der kantonale Datenschutzbeauftragte (KDSB) hat im Rahmen der Vorabkontrolle des Pilotprojekts der EKZ denn auch auf die Risiken für die Persönlichkeitsrechte der betroffenen Personen hingewiesen, welche mit dem Einsatz der neuen Messtechnik in Privathaushalten einhergehen. Insbesondere kritisierte der KDSB die vorgesehenen viertelstündlichen Messintervalle als unverhältnismässig kurz und wies auf die Gefahr hin, dass die Tagesabläufe in den Haushalten ausspioniert bzw. Persönlichkeitsprofile erstellt und die Daten anderen Nutzungsmöglichkeiten zugeführt werden könnten[65].

Das EWZ hat sich bereits im Rahmen der Planung der erwähnten Feldstudie mit dem städtischen Datenschutzbeauftragten in Verbindung gesetzt und in Zusammenarbeit mit ihm ein Datenschutzkonzept als verbindliche Grundlagen für die Feldstudie erstellt[66]. Dieses hält u.a. die Freiwilligkeit der Teilnahme am Forschungsprojekt sowie den Grundsatz der Datenbearbeitung in pseudonymiserter Form (welche nur Rückschlüsse auf die Zuordnung zu einer der fünf Vergleichsgruppen erkennen lässt) fest. Was die Datenbearbeitung in der Gruppe mit Smart Meter betrifft, so werden alle Daten der Smart Meter und Energieanzeigegeräte nur auf dem jeweiligen Gerät gespeichert; eine direkte Datenverbindung zum EWZ besteht nicht[67].

16 Passwort Reset mittels Biometrie

Bis heute müssen städtische Mitarbeitende, welche ihr Passwort für den Zugang zum IT-Büroarbeitsplatz vergessen haben, den Help Desk der OIZ in Anspruch nehmen. Mit der Einführung eines auf Spracherkennung und Stimmbiometrie basierenden, automatisierten Systems sollen die Mitarbei-

65 Vgl. dazu im Einzelnen NZZ vom 21. April 2010, S. 17 sowie TB KDSB 2009, S. 30. Mit Blick auf eine mögliche Erstellung von Persönlichkeitsprofilen hielt er zudem fest, dass die Zweckbindung der Datenerhebung – im Falle einer flächendeckenden Einführung von Smart Meters – ausdrücklich in einer gesetzlichen Grundlage festzuhalten sei.

66 Der Einsatz von Smart Meter ist im Projekt des EWZ – wie erwähnt – allerdings nur eine der Informationsmassnahmen, welche im Hinblick auf eine Senkung des Stromverbrauchs in Privathaushalten untersucht werden.

67 Die Geräte werden am Ende der Datenerhebung vor Ort abgeholt, vom ewz ausgelesen und in anonymisierter Form an die Universität Lausanne für die Auswertung weitergegeben.

tenden in Zukunft per Telefon die Rücksetzung ihrer Passwörter selber vornehmen können. Dies setzt voraus, dass sich die Mitarbeitenden in einem telefonischen Registrierungsprozess mit einer persönlichen Personalnummer identifizieren und dann fünf Zufallszahlen nachsprechen, wobei eine Spracherkennungssoftware prüft, ob die tatsächlich vorgegebenen Zahlen wiederholt worden sind. Dabei werden verhaltensbasierte Merkmale der Stimme sowie physische Merkmale des Stimmapparats ausgewertet und als sogenannte Voice Prints in einer zentralen Datenbank abgelegt. Die Stimme selber wird nicht aufgezeichnet. Nach einer solchen Registrierung können Nutzerinnen und Nutzer über die zentrale Telefonnummer des Systems die automatisierte Rücksetzung des vergessenen Passwortes veranlassen, wobei sie wie beim Registrierungsprozess einzelne Zufallszahlen nachsprechen müssen. Das biometrische System wertet die stimmbiometrischen Merkmale aus, vergleicht diese mit den im Rahmen der Registrierung extrahierten und gespeicherten stimmbiometrischen Merkmalen und setzt das Passwort bei identischen Voice Prints automatisch zurück.

Auf Grund der neuen Technologie des Systems sowie der grossen Anzahl der potentiell Nutzenden wurde das Vorhaben der Datenschutzstelle zur Vorabkontrolle angemeldet[68].

Im Fokus der Vorabkontrolle steht die Frage, ob mit den vorgesehenen Massnahmen die Anforderungen an die Informationssicherheit und Transparenz im Sinne von §§ 7 und 12 IDG erfüllt werden. Da beim geplanten Passwort Service der Stadt Zürich zudem biometrische Merkmale zentral gespeichert werden, sind erhöhte Anforderungen an die Informationssicherheit zu stellen[69]. Die Abklärungen bei der Projektleitung sowie beim Lieferanten liessen nach wie vor Fragen offen, insbesondere ob die Anforderungen an die Informationssicherheit bei der vorgesehenen Inbetriebsetzung erfüllt wären. Die Datenschutzstelle hat deshalb die IT-Security OIZ mit der Prüfung der technischen Massnahmen beauftragt. Zum Zeitpunkt der Drucklegung dieses Berichts lagen die Ergebnisse noch nicht vor.

68 Gemäss § 10 IDG muss eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung unterbreitet werden. Besondere Risiken liegen gemäss § 24 Abs. 1 IDV u.a. dann vor, wenn ein Vorhaben mit dem Einsatz neuer Technologien (lit. c) verbunden ist oder eine grosse Anzahl von Personen betrifft (lit. e).

69 Vgl. Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren von privatim, S. 15, wonach gefordert wird, dass biometrische Daten nicht in den Herrschaftsbereich des Systembetreibers, sondern in denjenigen der einzelnen Benutzenden gehören (bspw. in Form einer Chipkarten oder dgl).

17 Informationsaustausch im Bereich der Sozialhilfe

Der Vater einer Sozialhilfebezügerin wandte sich an die Datenschutzstelle, weil die Fürsorgebehörde der Stadt Zürich Auskünfte über seine finanziellen Verhältnisse bei der Steuerbehörde eingeholt hatte. Er konnte nicht verstehen, dass die Verwaltung Informationen über «unbescholtene Bürger» ohne deren Wissen und Einverständnis austauscht. Die Datenschutzstelle forderte die Fürsorgebehörde auf, zur Beschwerde eine schriftliche Stellungnahme abzugeben.

Sowohl das Schweizerische Zivilgesetzbuch[70] als auch das kantonale Sozialhilfegesetz[71] sehen die sog. Verwandtenunterstützungspflicht vor. Danach können Personen, die in günstigen finanziellen Verhältnissen leben, zur Unterstützung bestimmter, sich in Notlage befindlicher Angehöriger verpflichtet werden. Im Kanton Zürich ist die Prüfung dieser Unterstützungspflicht gesetzliche Pflicht der Fürsorgebehörden.[72] Diese sind somit nicht nur berechtigt, sondern sogar verpflichtet, die entsprechenden Abklärungen vorzunehmen und die hierfür erforderlichen Auskünfte (d.h. konkret das steuerbare Einkommen) einzuholen. Eine Einwilligung der betroffenen Personen ist für diese Auskunftserteilung nicht erforderlich.

Gestützt auf diese klare gesetzliche Ausgangslage hat die Datenschutzstelle dem eingangs erwähnten Vater die Auskunft erteilt, dass sich die involvierten Verwaltungsstellen korrekt verhalten haben und die Bekanntgabe der Informationen nicht zu beanstanden war.

Im Bereich der Sozialhilfe gibt es regelmässig Datenbekanntgaben, bei welchen sich die Frage nach Zulässigkeit und Umfang nicht so klar beantworten lassen wie im geschilderten Sachverhalt. Prominentestes Beispiel war wohl die vor einigen Jahren breit geführte Debatte, ob und unter welchen Voraussetzungen Verwaltungsstellen bei Verdacht auf Sozialhilfemissbrauch von sich aus Meldung an die Sozialhilfebehörde machen dürfen. Da zum damaligen Zeitpunkt keine genügende gesetzliche Grundlage (insbesondere auf kantonaler Ebene) vorhanden war, erliess der Stadtrat im Februar 2008 einen Beschluss, welcher die städtischen Verwaltungsbehörden zu entsprechenden Meldungen an das Sozialdepartement ermächtigte.[73]

70 Art. 328 und 329 ZGB; SR 210.

71 §§ 25 ff. SHG; LS 851.1.

72 § 25 Abs. 1 SHG.

73 AS 851.120; vgl. auch TB 2007 S. 5 f. Der Stadtrat wies bereits damals darauf hin, dass die neue kommunale Rechtsnorm eine Übergangslösung darstelle und nur solange in Kraft stehe, bis entsprechende kantonale Vorschriften erlassen werden.

Im Herbst 2009 beantragte der Regierungsrat des Kantons Zürich eine Teilrevision des kantonalen Sozialhilfegesetzes[74], welche Änderungen und Präzisierungen v.a. bezüglich Informationsaustausch zwischen den verschiedenen involvierten Amtsstellen und Behörden, aber auch bezüglich der Auskunftspflicht von Dritten zum Gegenstand hat.[75] Der Kantonsrat hat die Revision des kantonalen Sozialhilfegesetzes am 12. Juli 2010 gutgeheissen. Nachdem gegen die Vorlage das Referendum (mit Gegenvorschlag von Stimmberechtigten) ergriffen wurde[76], kommt sie allerdings noch zur Abstimmung.[77]

18 Analyse der Wählerinnen und Wähler

Statistik Stadt Zürich erstellte und publizierte eine Analyse der Wählerinnen und Wähler, die an den National- und Ständeratswahlen vom Oktober 2007 teilgenommen hatten[78], nach verschiedenen soziodemografischen Merkmalen (Geschlecht und Alter, Zivilstand, Einkommen und Vermögen, Aufenthaltsdauer in der Stadt). Im Nachgang zu dieser Publikation wurde im Gemeinderat ein Postulat eingereicht, mit welchem der Stadtrat um Prüfung gebeten wurde, wie bei Wahlen und Abstimmungen auf Datenerhebungen in der Stadt Zürich verzichtet werden kann.[79] Das Postulat wurde an der Gemeinderatssitzung vom 15.12.2010 abgelehnt. Im Zusammenhang mit dem erwähnten Postulat hat sich eine Gemeinderätin an die Datenschutzstelle gewandt und um eine datenschutzrechtliche Beurteilung derartiger Analysen von Wählerinnen und Wählern gebeten.

Das kantonalzürcherische Datenschutzrecht beinhaltet den Grundsatz, dass die Verwaltung ihre Informationen zu Forschungs-, Planungs- oder Statistikzwecken (sog. nicht personenbezogenen Zwecken) auswerten darf, sofern dies nicht durch eine rechtliche Bestimmung ausgeschlossen ist, die Daten baldmöglichst anonymisiert werden und die Auswertungen keine Rückschlüsse auf betroffene Personen ermöglichen[80]. Allfällige rechtliche Bestimmungen, welche eine statistische Auswertung von Informationen oder die Bekanntgabe von Informationen zu Statistikzwecken (bspw. an externe Forschungsinstitute) verbieten könnten, sind in den jeweiligen Spezialgesetzen zu suchen. Eine solche spezialgesetzliche Grundlage ist vorliegend das kantonale Gesetz über die politischen Rechte[81]. § 8 Abs. 2 dieses Gesetzes bestimmt, dass es unter «Wahrung des Stimmgeheimnisses» zulässig ist, das Stimmverhalten der Bevölkerung auszuwerten und zu veröffentlichen. Vorliegend beinhaltet die Spezialgesetzgebung also kein Verbot, son-

74 KR-Nr. 4628/2009.

75 Geregelt werden bspw. die Meldepflicht der Sozialhilfeorgane an die Ausländerbehörden, die Meldepflicht und Amtshilfe von Verwaltungsbehörden an die Sozialhilfeorgane sowie die Auskunftserteilung durch die Sozialhilfeorgane.

76 Die neuen Bestimmungen hinsichtlich Informationsaustausch und Auskunftserteilung (Fn 75) waren im Gesetzgebungsprozess nicht grundsätzlich umstritten und sind auch nicht Gegenstand des Gegenvorschlags.

77 Geplanter Abstimmungstermin ist der 4. September 2011.

78 «Wer geht an die Urne?», Soziodemografisches Profil der Wählenden bei den National- und Ständeratswahlen 2007, aus der Publikationsreihe «Zur Zeit», Ausgabe 1/2007.

79 GR Nr. 2007/583.

80 §§ 9 und 18 IDG.

81 GPR, LS 161.

dern lässt im Gegenteil sogar ausdrücklich die Auswertung und Publikation des Stimmverhaltens zu. Dies allerdings unter dem Vorbehalt, dass Dritte vom Inhalt der Stimme keine Kenntnis erhalten dürfen und dass der Inhalt der Stimme nicht der stimmberechtigten Person zugeordnet werden kann. Was die erwähnte Analyse der National- und Ständeratswahlen 2007 betrifft, wurden Ablauf und Modalitäten vorgängig vom Stadtrat verbindlich definiert und von der Datenschutzstelle geprüft. Dabei gab es keinerlei Anhaltspunkte dafür, dass die Wahrung des Stimmgeheimnisses und die erforderliche Anonymisierung nicht vollumfänglich eingehalten oder durch die Publikation unzulässige Rückschlüsse auf betroffene Personen ermöglicht worden wären.

19 Geheimhaltungsverpflichtung (Mustervorlage)

Gemäss bisheriger Praxis haben Mitarbeitende der Stadtverwaltung bei Stellenantritt einen sog. Revers zu unterzeichnen, mit welchem sie auf die geltenden Geheimhaltungspflichten, namentlich das Amtsgeheimnis und den Datenschutz, hingewiesen werden. Angesichts der gesetzlichen Ausgangslage, wonach Verwaltungsangestellte ohnehin gesetzlichen Geheimhaltungspflichten unterstellt sind[82], ist nach Auffassung der Datenschutzstelle Sinn und Nutzen eines solchen von Mitarbeitenden (zusätzlich) zu unterzeichnenden Revers nicht erkennbar. Auch ergibt sich weder aus Personal- noch Datenschutzrecht eine Rechtsgrundlage, welche die Unterzeichnung eines derartigen Revers für Mitarbeitende als obligatorisch vorschreibt.

Auch eine von der Datenschutzstelle durchgeführte Umfrage zum Thema «Geheimhaltungspflichten (bzw. Schweigepflichten oder Datenschutzrecht) für Verwaltungsangestellte» bei verschiedenen Kantons- und Stadtverwaltungen in der Deutschschweiz hat gezeigt, dass die meisten Verwaltungen auf die Unterzeichnung einer Geheimhaltungserklärung verzichten und anstelle eines solchen «Formalismus» den Schwerpunkt auf die Sensibilisierung der Mitarbeitenden legen. Von Seiten der Datenschutzstelle wird ein solcher Revers denn auch nicht weiter verlangt[83] und dementsprechend auch nicht mehr auf der Website als Muster zur Verfügung gestellt.

82 Neben der strafrechtlichen Sanktionierung bei Verletzung des Amtsgeheimnisses gemäss Art. 320 StGB ist das Amtsgeheimnis regelmässig Gegenstand personalrechtlicher Bestimmungen, für die Stadtverwaltung Zürich bspw. in Art. 80 PR.

83 Im Rahmen der Abklärung über die Bereitstellung von Muster-Revers und -Geheimhaltungen wurde aber deutlich, dass HRZ an einem Revers für Mitarbeitende festhalten möchte und ein überarbeitetes Formular künftig in SAP und im HRZ-Intranet bereitstellen wird.

Anders beurteilte die Datenschutzstelle die Nachfrage nach einem Muster für eine Geheimhaltungsverpflichtung für Dritte. Die Bereitstellung einer solchen Vorlage drängte sich angesichts des am 1. Oktober 2008 in Kraft getretenen kantonalen Gesetzes über die Information und den Datenschutz (IDG) geradezu auf, da dieses bei Outsourcing verlangt, dass die Auftragserteilung an Dritte (d.h. an verwaltungsexterne Stellen oder Personen) schriftlich geregelt wird und Gegenstand dieser schriftlichen Vereinbarung auch eine Geheimhaltungsverpflichtung sein muss (§ 6 IDG; § 25 IDV).

Seit März 2010 steht das in Zusammenarbeit mit der OIZ überarbeitete Muster für eine Geheimhaltungsvereinbarung mit Dritten wieder elektronisch zur Verfügung. Die Datenschutzstelle weist auf ihrer Website allerdings ausdrücklich darauf hin, dass von einer pauschalen Übernahme des Muster-Textes abzusehen und eine Anpassung auf die konkreten Gegebenheiten und Bedürfnisse vorzunehmen ist[84].

20 Auskunft über Verstorbene

Die Stadtpolizei hatte das Gesuch eines Sohnes um Einsicht in die Akten seines verstorbenen Vaters mit Verweis auf den Datenschutz abgelehnt. Der im Ausland wohnhafte Sohn wandte sich daraufhin an die Datenschutzstelle, welche ihrerseits die Stadtpolizei um eine schriftliche Begründung der Auskunftsverweigerung bat. Die Stadtpolizei begründete diese damit, dass weder einer der in § 17 IDG[85] abschliessend aufgelisteten Gründe vorliege, noch die Polis-Verordnung[86] eine Bestimmung enthalte, welche die Auskunft im vorliegenden Fall vorsehen würde. Auf den ersten Blick erschien die Begründung der Stadtpolizei zwar nachvollziehbar und korrekt, dennoch kam die Datenschutzstelle aufgrund folgender Überlegungen zu einer anderen Beurteilung des erwähnten Gesuchs um Einsicht in die Akten eines Verstorbenen:

Betroffene Personen im Sinne der Datenschutzgesetzgebung können nur Personen sein, die noch existieren, d.h. natürliche Personen, die noch leben[87]. Daraus folgt, dass sich ein allfälliger Informationsanspruch über eine verstorbene Person nicht auf das Auskunftsrecht gemäss § 20 Abs. 2 IDG (datenschutzrechtliches Auskunftsrecht über eigenen Personendaten), sondern immer nur auf § 20 Abs. 1 IDG (Zugangsrecht aus Öffentlichkeitsprinzip) stützen kann. Die Unterscheidung, ob § 20 Abs. 1 oder Abs. 2 IDG die massgebende Grundlage darstellt, mag zunächst wie eine blosse juristi-

84 Im Einzelfall kann es angezeigt sein, bestimmte Regelungen wegzulassen, anders zu formulieren oder zu erweitern. Allenfalls können auch die Bestimmungen des städtischen Reglements Remote Support und insbesondere die dazugehörigen Allgemeinen Geschäftsbedingungen herangezogen werden, welche auch Regelungen zur Geheimhaltung enthalten.

85 § 17 IDG regelt die Bekanntgabe besonderer Personendaten. Das öffentliche Organ darf besondere Personendaten u.a. bekannt geben, «wenn eine hinreichend bestimmte Regelung in einem formellen Gesetz dazu ermächtigt».

86 LS 551.103.

87 Das schweizerische Recht kennt keinen sog. postmortalen Persönlichkeitsschutz, d.h. eine verstorbene Person besitzt keine Rechtsfähigkeit mehr und kann ihre Rechte daher auch nicht vertretungsweise durch die Angehörigen oder andere Dritte geltend machen.

sche Spitzfindigkeit erscheinen. Dass sie es aber nicht ist, machen die praktischen Konsequenzen deutlich, welche die Unterscheidung für den konkret zu beurteilenden Fall haben. Wird § 20 Abs. 2 IDG als massgebend erachtet, so müsste festgestellt werden, dass dem Sohn bereits dem Grundsatz nach keine Auskunft erteilt werden darf, da die Informationen über den verstorbenen Vater keine eigenen (d.h. den Sohn betreffenden) Personendaten darstellen. Wird dahingegen von § 20 Abs. 1 IDG ausgegangen, so ist ein Informationsrecht dem Grundsatz nach gegeben und das konkrete Gesuch einer Interessenabwägung zu unterziehen.

§ 20 Abs. 1 IDG gibt jeder Person Anspruch auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen. Dieses Zugangsrecht kann grundsätzlich auch Personendaten beinhalten, welche Drittpersonen betreffen. Inwieweit eine Auskunft erteilt werden und in welchem Masse diese Auskunft auch Personendaten umfassen kann, hat die angefragte Verwaltungsstelle für jeden Einzelfall anhand einer Interessenabwägung zu klären[88].

Im Falle von Auskünften über verstorbene Personen ging der Gesetzgeber davon aus, dass ein berechtigtes Interesse für die Auskunftserteilung bei nahen Verwandten (Kinder, Eltern) gegeben ist[89]. Stand der Gesuchsteller zur verstorbenen Person nicht in einem nahen Verwandtschaftsverhältnis, darf Auskunft nur erteilt werden, wenn ein besonderes Interesse nachgewiesen wird und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen.[90]

Für Auskünfte über Verstorbene stellt somit nach Auffassung der städtischen Datenschutzstelle § 20 Abs. 1 IDG die allgemeine gesetzliche Grundlage dar. Da die Frage, in welchem Umfang vorliegend dem Gesuchsteller letztlich Informationen bekannt zu geben sind, nur in Würdigung der konkreten Umstände entschieden werden kann, gab die Datenschutzstelle der Stadtpolizei die Empfehlung, die entsprechende Interessenabwägung vorzunehmen und – abhängig vom Resultat dieser Interessenabwägung – dem Sohn die verlangten Auskünfte zu geben[91]. Die Stadtpolizei Zürich erteilte dem Sohn schliesslich die gewünschte Einsicht in ihre Akten.

88 § 23 IDG.

89 Nebst «naher Verwandtschaft» begründen auch «im Zeitpunkt des Versterbens bestehende Ehe, eingetragene Partnerschaft und eheähnliche Lebensgemeinschaft mit der verstorbenen Person» ein Interesse an der Auskunftserteilung (§ 19 IDV). Diese gesetzliche Vermutung entbindet allerdings nur die gesuchstellende Person vom Interessennachweis, nicht aber das zuständige Organ von der Interessenabwägung. § 19 IDV hält denn auch ausdrücklich fest, dass das zuständige Organ bei einem solchen Gesuch zusätzlich prüfen muss, ob der Auskunft anderweitige Interessen von Angehörigen oder Dritten entgegenstehen.

90 Festzuhalten ist, dass die Gesetzessystematik von § 19 IDV unzutreffend ist. § 19 IDV kann aus naheliegenden Gründen nicht den Zugang (eines Verstorbenen) zu eigenen Personendaten regeln (so aber der Titel zu §§ 16 ff. IDV und der dortige Verweis auf § 20 Abs. 2 IDG), sondern nur auf das Dritten zustehende Informationszugangsrecht (§ 20 Abs. 1 IDG) anwendbar sein.

91 Für die Entscheidung im Einzelfall ist die Interessenabwägung nach § 23 IDG entscheidend, wobei einer Auskunft namentlich keine polizeilichen Interessen und keine überwiegenden Interessen von Angehörigen oder Dritten entgegenstehen dürfen (§ 19 IDV).

21 Drittmeldepflicht der Vermieter

Wer sich in einer Gemeinde über einen bestimmten Zeitraum aufhält oder Wohnsitz nimmt, muss sich bei der Einwohnerkontrollbehörde anmelden. Zur Sicherstellung dieser Meldepflicht besteht im Kanton Zürich eine gesetzlich statuierte Drittmeldepflicht der Vermieter (worunter auch die Liegenschaftenverwaltungen zu verstehen sind).[92] In der Stadt Zürich können die Vermieter dem für die Einwohnerkontrolle zuständigen Personenmeldeamt die Ein- und Auszüge von Mieterinnen und Mietern elektronisch über das Internet melden.

Das Meldewesen der Einwohnerkontrollbehörden soll in der Schweiz durch die Einführung standardisierter, elektronischer Ein- und Auszugsanzeigen vereinheitlicht werden. Eine entsprechende Fachgruppe des Vereins eCH[93] erarbeitet diesbezügliche Standards und Hilfsmittel. Im Rahmen dieser Arbeiten war umstritten[94], ob Einwohnerkontrollbehörden standardmässig die Mitteilung von Staatsangehörigkeit und Geburtsdatum der Mieterschaft – so wie dies in der Stadt Zürich über die Internetmeldungen bereits seit längerem Praxis ist – verlangen dürfen. Das Personenmeldeamt hat deshalb die Datenschutzstelle der Stadt Zürich um eine diesbezügliche Beurteilung gebeten.

Für die Drittmeldepflicht der Vermieter besteht im Kanton Zürich[95] im Gemeindegesetz die notwendige Rechtsgrundlage. Der Inhalt der Drittmeldepflicht ist nicht abschliessend festgelegt. Der Gesetzgeber hat den Einwohnerkontrollbehörden einen gewissen Ermessensspielraum eingeräumt. Da es sich bei den Datenfeldern Staatsangehörigkeit und Geburtstag im Rahmen der Drittmeldepflicht um nicht sensible Personendaten handelt, ist eine Bearbeitung dieser Informationen zulässig, wenn sie zur Erfüllung der gesetzlichen Aufgaben geeignet und erforderlich sind[96]. Gemäss Auskunft des Personenmeldeamtes der Stadt Zürich ist das Geburtsdatum für die eindeutige Identifizierung der (säumigen) meldepflichtigen Mieterinnen und Mieter wichtig. Die Kenntnis der Staatsangehörigkeit sei relevant, weil die Mieterinnen und Mieter je nach Nationalität für die Anmeldung sowohl unterschiedliche Dokumente vorlegen, als auch unterschiedliche Gebühren bezahlen müssen. Bei Kenntnis der Staatsangehörigkeit könnten die Ein-

92 §§ 32 ff. Gemeindegesetz des Kantons Zürich, LS 131.1.

93 Der Verein eCH fördert, entwickelt und verabschiedet Standards im Bereich E-Government. Die Trägerschaft von eCH bilden Bund, Kantone, Städte und Gemeinden sowie Wirtschaft und Wissenschaft. Das Personenmeldeamt der Stadt Zürich ist in der entsprechenden Fachgruppe Meldewesen des Vereins eCH vertreten; www.ech.ch.

94 Zur diesbezüglichen Zulässigkeit vertritt bspw. der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte eine kritische Haltung.

95 Das Einwohnerkontrollwesen fällt in die kantonale Gesetzgebungskompetenz. Bei der Erarbeitung eines schweizweiten Standards ist deshalb zu berücksichtigen, dass sich die Modalitäten der Meldepflichten nach den jeweiligen kantonalen Rechtsgrundlagen beurteilen.

96 § 8 Abs. 1 IDG.

97 Die Drittmeldepflicht hat für die Vermieter nicht zur Folge, dass sie bei der Mieterschaft zusätzliche Informationen erheben müssen. Es kann aber davon ausgegangen werden, dass die Vermieter im Zeitpunkt des Abschlusses eines Mietvertrages und damit im Zeitpunkt, in welchem die Drittmeldepflicht ansetzt, über die entsprechenden Informationen verfügen.

98 GRB 1106, GR Nr. 2006/303.

wohnerkontrollbehörden den Mieterinnen und Mietern bereits bei der Einladung mitteilen, welche Unterlagen sie mitbringen müssen und welche Gebühren anfallen. In Anbetracht des Nutzens, den diese Informationen für die Kontrollaufgaben des Personenmeldeamtes haben sowie unter Berücksichtigung, dass diese Informationen der Einwohnerkontrolle bei der Anmeldung durch die Mieterinnen und Mieter bekannt gegeben werden müssen, beurteilt die Datenschutzstelle das Verfahren des Personenmeldeamtes als datenschutzkonform. Die Vermieter sind im Rahmen der Ein- und Auszugsanzeigen somit zur Bekanntgabe dieser Informationen grundsätzlich verpflichtet, jedoch nur, sofern sie über diese Informationen bereits verfügen[97].

22 Case Management am Arbeitsplatz

Evaluation und Schlussbericht

Der Gemeinderat hat im Beschluss bezüglich der Einführung von Case Management am Arbeitsplatz verlangt, dass ihm der Stadtrat im Jahre 2010 Bericht über die mit Case Management gemachten Erfahrungen erstattet und Antrag über die Weiterführung stellt[98]. Für diese Berichterstattung hat HRZ eine umfassende Evaluation des Case Managements vorgenommen. Neben der statistischen Auswertung des bestehenden Datenmaterials wurden für die Evaluation zusätzlich weitere statistische Erhebungen bei den an der Durchführung beteiligten Personen und Stellen durchgeführt. Der Datenschutzstelle wurde ein Entwurf des Schlussberichtes zur Prüfung und Stellungnahme vorgelegt.

Die Datenschutzstelle hat HRZ die datenschutzrechtlichen Rahmenbedingungen dargelegt, welche bei Evaluation und Berichterstattung erfüllt werden müssen. Bei der Prüfung des vorgelegten Entwurfs richtete die Datenschutzstelle ein spezielles Augenmerk auf die Informationen über die im Case Management erfassten Krankheiten und deren Verteilung in der Stadtverwaltung. Dabei hat die Datenschutzstelle festgestellt, dass einzelne Auswertungen so detailliert waren, dass Rückschlüsse auf einzelne Personen (insbesondere bei entsprechendem Insiderwissen) nicht ausgeschlossen werden konnten. Die Datenschutzstelle hat HRZ auf diese Problematik hingewiesen und empfohlen, die Sicherstellung der Anonymisierung nochmals zu überprüfen und allfällige Anpassungen vorzunehmen. Die Empfehlungen

des Datenschutzbeauftragten wurden im Vernehmlassungsentwurf des Stadtrats[99] umgesetzt. Der Gemeinderat hat vom Bericht des Stadtrats mit Beschluss vom 22. Dezember 2010 zustimmend Kenntnis genommen und der definitiven Weiterführung von Case Management am Arbeitsplatz zugestimmt.[100]

e-Case

Für die Bearbeitung der Case Management-Anmeldungen und der elektronischen Klientendossiers wird in der Stadtverwaltung das Standardprogramm e-Case eingesetzt. Da die Case Managerinnen und Case Manager verschiedener Departemente und grösserer Dienstabteilungen an dieses zentrale System angeschlossen sind und die Fallbearbeitung im Case Management die Bearbeitung höchst sensibler Personendaten umfasst, sind an ein solches System und insbesondere an die Regelung der Zugriffsberechtigungen erhöhte Anforderungen zu stellen. Bei der Überprüfung von e-Case hat die Datenschutzstelle verschiedene Defizite festgestellt. Insbesondere fehlte ein verbindliches Zugriffs- und Berechtigungskonzept. Andererseits waren die zu Supportzwecken notwendigen Zugriffe[101] nicht genügend kontrollierbar. Auf Empfehlung der Datenschutzstelle hat die Projektleitung Case Management die mit der Anwendung e-Case verbundenen Risiken durch die IT-Security OIZ genauer untersuchen und im Rahmen eines ISDS-Konzepts[102] die entsprechenden Massnahmen formulieren lassen. Als zentrale Massnahme wurde der Erlass eines restriktiven Zugriffs- und Berichtigungskonzepts verlangt. Zur Behebung der bisher mangelhaften Kontrollierbarkeit der zu Supportzwecken notwendigen Zugriffe wurde einerseits der Verzicht auf Fernwartung und andererseits die Implementierung einer Desktop-Sharing-Lösung[103] vorgesehen.

Gestützt auf das in der Zwischenzeit der Datenschutzstelle vorgelegte Zugriffs- und Berechtigungskonzept[104] sowie der weiteren umgesetzten Massnahmen konnte die Datenschutzstelle den Einsatz der Anwendung e-Case als datenschutzkonform beurteilen.

99 StRB 507, vom 24.3.2010.

100 GRB 925, GR NR. 2010/329.

101 Der Support erfolgt primär durch andere Case Managerinnen und Case Manager der Stadtverwaltung, welche hierfür teilweise Zugriff bis auf Ebene Falldossier benötigen.

102 Informationssicherheits- und Datenschutz-Konzept.

103 Zugriffe zu Supportzwecken erfolgen nur mit Einwilligung der Fallverantwortlichen Case Managerinnen und Case Manager. Die Zugriffe können am Bildschirm verfolgt und damit kontrolliert werden.

104 Dieses gewährt lediglich den für einen bestimmten Fall zuständigen Case Managerinnen und Case Manager sowie deren Stellvertretung Zugriff auf das entsprechende Falldossier.

[105] Art. 141 ABPR.

[106] Gegenstand der Beurteilung bilden insbesondere Arbeitsführung, Arbeitsergebnisse, Selbständigkeit, Verhalten, Erreichen der vereinbarten Ziele sowie – bei Vorgesetzten – die Führungstätigkeit.

[107] Leitfaden allgemeine Grundlagen sowie Leitfaden für Vorgesetzte.

23 Zielvereinbarungs- und Beurteilungsgespräche

Jährlich führen die Vorgesetzten in der Stadtverwaltung mit ihren Mitarbeitenden Zielvereinbarungs- und Beurteilungsgespräche (ZBG) durch. Zweck und Umfang dieser Gespräche sind im Personalrecht geregelt[105]. Dieses bestimmt, dass mit den ZBG das Personal zu fördern und Leistung und Verhalten der Mitarbeitenden zu beurteilen sind[106]. Im Personalrecht nicht erwähnt und bisher nicht Gegenstand der ZBG war die Gesundheitsförderung. Diese soll in der Stadtverwaltung im Rahmen der ZBG neu als Führungsaufgabe berücksichtigt werden. Im Berichtsjahr hat HRZ einen entsprechenden Weisungsentwurf zusammen mit neu überarbeiteten Leitfäden[107] in die Vernehmlassung geschickt. In diesen Leitfäden werden die Vorgesetzten u.a. ausdrücklich dazu angehalten, den Mitarbeitenden Fragen zu ihrer Gesundheit zu stellen.

Die Datenschutzstelle hat HRZ in ihrer Stellungnahme darauf aufmerksam gemacht, dass aus den Leitfäden weder hervorginge, unter welchen konkreten Voraussetzungen und zu welchem Zweck Fragen zur Gesundheit überhaupt zulässig seien, noch ob und wie der Arbeitgeber solche Informationen bearbeiten dürfe.

Zudem hat die Datenschutzstelle in ihrer Stellungnahme auch darauf hingewiesen, dass sie für die Einführung der Gesundheitsförderung im Rahmen von ZGB eine Ergänzung der massgebenden Bestimmung des Personalrechts für notwendig erachte. HRZ hat im Anschluss an das Vernehmlassungsverfahren die Stadtratsweisung und die zugehörigen Leitfäden dahingehend präzisiert, dass Fragen zu gesundheitlichen Themen nur dann zulässig sind, wenn sich diese auch auf das Arbeitsverhältnis auswirken oder auswirken können. Auch wird festgehalten, dass bei den ZBG-Schulungen den datenschutzrechtlichen Fragen, insbesondere im Hinblick auf die Gesundheitsförderung, besondere Beachtung geschenkt werde. Mit der Stadtratsweisung (noch) nicht in die Wege geleitet wurde die von der Datenschutzstelle im Vernehmlassungsverfahren angeregte Ergänzung des Personalrechts.

24 Auswertungen von Mitarbeiterdaten zu Qualitäts- und Produktivitätskontrollen

Die Verkehrsbetriebe der Stadt Zürich (VBZ) setzen für Fahrausweiskontrollen ein sog. Fahrausweiskontrollsystem (FAKS-System) ein. Im Rahmen dieses Systems muss das Kontrollpersonal alle seine Tätigkeiten während eines Arbeitstages mit mobilen Erfassungsgeräten erfassen (wie bspw. kontrollierte Fahrzeuge, Zuschläge bei Fahrgästen ohne Billet, Fahrdiensteinsätze oder Pausen). Diese Daten werden für das Taxzuschlagswesen, für die Erfassung der Arbeitszeit der Kontrolleure sowie für statistische Auswertungen bearbeitet. Mitarbeiterbezogene Auswertungen werden gemäss Auskunft der VBZ nur ausnahmsweise und nur dann vorgenommen, wenn ein konkreter, begründeter Anlass besteht (bspw. bei glaubhaften Zweifeln an der vorschriftgemässen Pflichterfüllung eines Mitarbeitenden). Diese bisherige Praxis der VBZ wurde von der Datenschutzstelle bereits einmal überprüft und als datenschutzkonform beurteilt.

Die VBZ sind nun dazu übergegangen, stichprobenweise die Arbeitsrapporte der Teams auszuwerten und mit diesen (in anonymisierter Weise) zu besprechen. Diese Auswertungen erfolgen in erster Linie zu Qualitätskontrollzwecken[108], können aber ausnahmsweise, wenn bei solchen Stichproben Verfehlungen von einzelnen Mitarbeitenden entdeckt werden, für diese personalrechtliche Konsequenzen haben. Mitarbeitende der VBZ ersuchten die Datenschutzstelle um eine datenschutzrechtliche Beurteilung dieser Praxisänderung. Sie bezweifelten die Rechtmässigkeit der Auswertungen und bemängelten, dass die Mitarbeitenden über die Auswertungen und die damit verbundenen personalrechtlichen Konsequenzen nicht genügend informiert seien.

Die Datenschutzstelle hat die Auswertungen zu Qualitätskontrollzwecken der VBZ überprüft und grundsätzlich als zulässig beurteilt. Zu kritisieren war jedoch die mangelhafte Sicherstellung, dass die Kontrollen und Auswertungen nur zu den deklarierten Qualitätskontrollen veranlasst bzw. durchgeführt werden. Inzwischen haben die VBZ auf Empfehlung der Datenschutzstelle die erforderlichen organisatorischen Anpassungen vorgenommen. Auch haben die VBZ das Informationsdefizit den Mitarbeitenden gegenüber erkannt und diese über die Voraussetzungen für Auswertungen sowie das Vorgehen und die Rechte der Mitarbeitenden bei Auswertungen aus dem FAKS-System schriftlich orientiert.

[108] Gemäss VBZ können mit solchen Kontrollen Rückschlüsse auf mögliche Prozess- und Effizienzverbesserungen der Kontrollgruppen gezogen werden.

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

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

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

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

Monika Niederberger
Sekretariat (20 %)

Viviane Kull, lic.iur.
Rechtspraktikantin

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