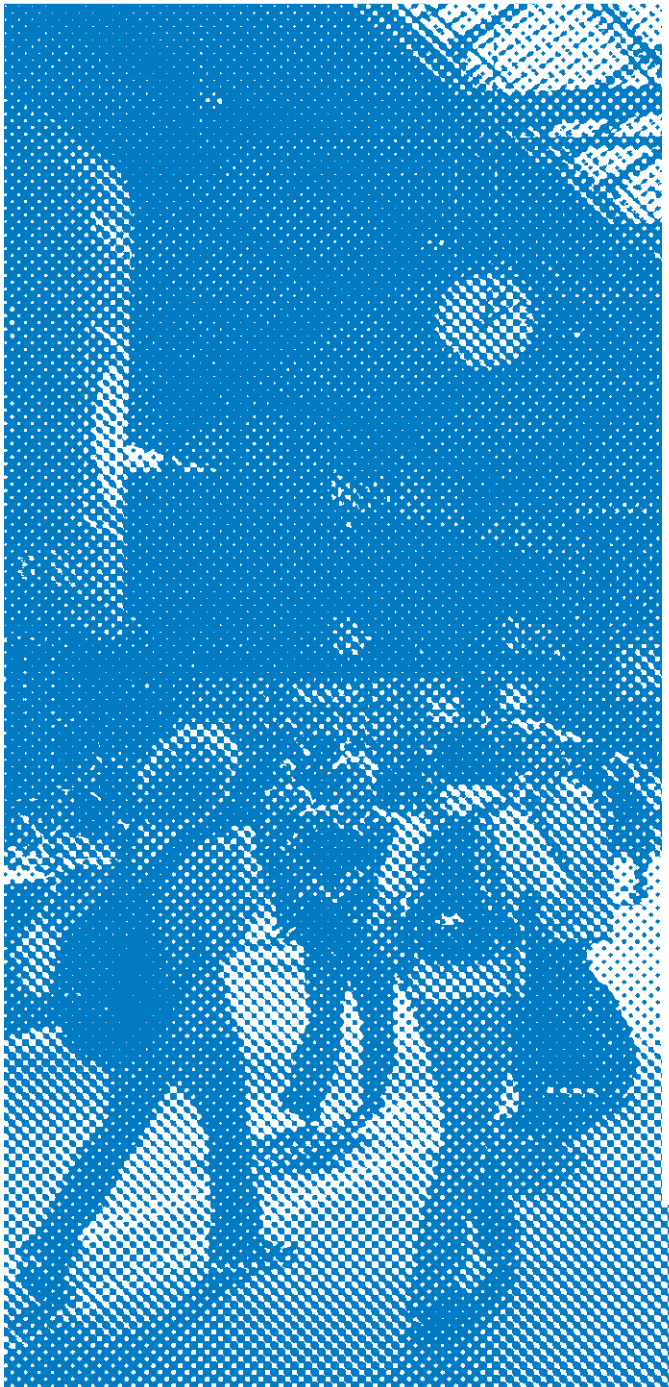
Stadt Zürich
Datenschutzbeauftragter

Tätigkeitsbericht 2011



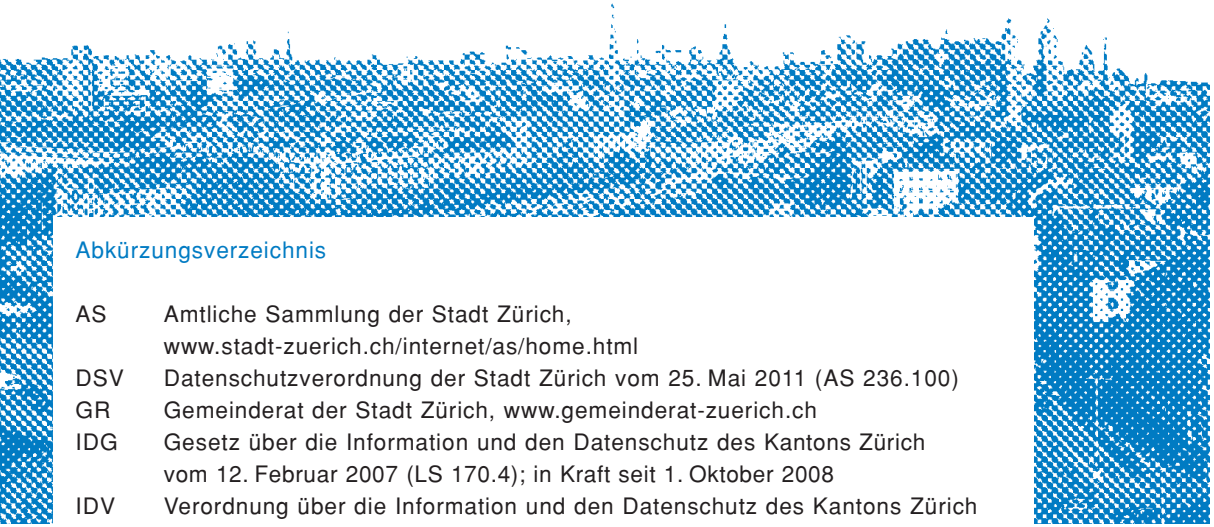
Der Datenschutzbeauftragte hat dem Stadtrat und dem Gemeinderat jährlich einen Bericht über Tätigkeit und Feststellungen und über den Stand des Datenschutzes zu erstatten*.

Der vorliegende Tätigkeitsbericht deckt den Zeitraum von 1. Januar 2011 bis 31. Dezember 2011 ab.

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

*§ 39 IDG

Inhaltsverzeichnis



Abkürzungsverzeichnis

AS	Amtliche Sammlung der Stadt Zürich, www.stadt-zuerich.ch/internet/as/home.html
DSV	Datenschutzverordnung der Stadt Zürich vom 25. Mai 2011 (AS 236.100)
GR	Gemeinderat der Stadt Zürich, www.gemeinderat-zuerich.ch
IDG	Gesetz über die Information und den Datenschutz des Kantons Zürich vom 12. Februar 2007 (LS 170.4); 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

I Berichtsjahr 2011

Ausgeprägter als in früheren Jahren standen im Berichtsjahr 2011 konzeptionelle Arbeiten wie bspw. die Erarbeitung von Vorlagen oder die Definition von Prozessen im Zentrum der Tätigkeiten der Datenschutzstelle. Zurückzuführen ist dies in erster Linie auf neue oder fehlende Rechtsgrundlagen oder aber auf sich verändernde informationstechnische Anforderungen an die Verwaltung:

– Die revidierte städtische Datenschutzverordnung (DSV) enthält erstmals spezifische Rechtsgrundlagen zur Videoüberwachung. Regelungen auf Gesetzesstufe bringen es mit sich, dass sie abstrakt formuliert sind und für eine einheitliche Anwendung in der Praxis erst noch konkretisiert werden müssen (Bericht Nr. 1).

– Die Vorschriften zur Vorabkontrolle gemäss kantonalem Informations- und Datenschutzgesetz (IDG) sind zwar etwas älter, aber nicht weniger konkretisierungsbedürftig. Ein wichtiger Schritt in diese Richtung ist die Erarbeitung einer Vorlage für ein städtisches Informationssicherheits- und Datenschutzkonzept (Bericht Nr. 6).

– Das Fehlen notwendiger Regelungen ist Grund für die konzeptionellen Arbeiten der Datenschutzstelle in Bezug auf den Umgang mit sog. Rand- oder Verkehrsdaten. Der moderne Arbeitsplatz wird je länger je mehr beherrscht durch elektronische Geräte und Infrastrukturen, bei deren Nutzung unvermeidbar auch Personendaten anfallen. Erforderlich sind klare und transparente Nutzungs- und Überwachungs(spiel)regeln. Hierfür hat eine Arbeitsgruppe unter der Leitung der Datenschutzstelle einen Entwurf für ein entsprechendes Reglement erarbeitet. Gegenstand des Tätigkeitsberichts soll dieses Reglement erst nächstes Jahr werden, wenn die Ergebnisse der stadtinternen Vernehmlassung, welche der Stadtrat bis Mitte Juli 2012 angesetzt hat, vorliegen.

– An die Verwaltung werden auch informationstechnisch immer neue Anforderungen gestellt. Hinter Begriffen wie «Open Government Data» oder «Service-orientierte Architektur» stehen neue Verfahren, die eine Vielzahl von Datenbearbeitungen aus unterschiedlichen Verwaltungsbereichen tangieren und umfassen. Auch hier investierte die Datenschutzstelle vor allem in die Erarbeitung der erforderlichen Prozesse und Abläufe (Berichte Nr. 5 und 7).

Die weiteren Berichte geben Einblick in die Prüfungs- und Beratungstätigkeiten sowohl in Bezug auf Projekte und Vorhaben aus der Stadtverwaltung als auch in Bezug auf die zahlreichen Einzelanfragen seitens Verwaltung und Bevölkerung der Stadt Zürich.

II Themen

1 Videoüberwachung

Mit dem Inkrafttreten der Datenschutzverordnung (DSV)[1] auf den 1. Oktober 2011 sind auch die Bestimmungen über Videoüberwachung[2] in Kraft getreten. Um den Verantwortlichen[3] die notwendigen Abklärungen zu erleichtern, ob eine Videoüberwachungsanlage überhaupt den gesetzlichen Anforderungen entspricht und somit zulässig ist und um sie bei der Ausarbeitung eines Reglements zu unterstützen, hat die Datenschutzstelle verschiedene Hilfsdokumente erarbeitet und im Internet veröffentlicht[4].

Nebenstehendes Ablaufschema gibt eine Übersicht über das Vorgehen bei einer (geplanten oder bereits betriebenen) Videoüberwachung:

Aufgrund der gesetzlichen Bestimmungen ist zunächst immer abzuklären, ob

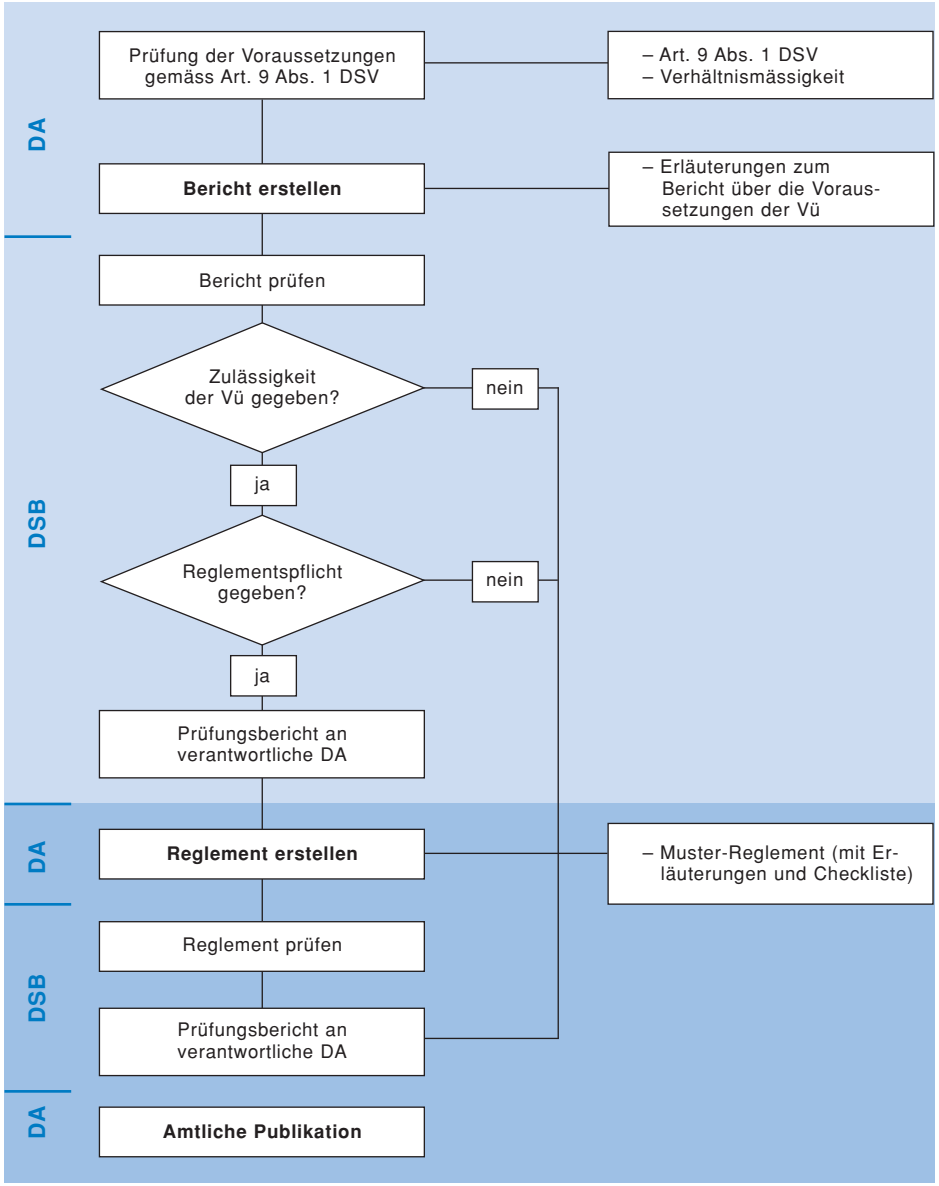
- die gesetzlichen Voraussetzungen des Art. 9 Abs. 1 DSV («erhebliche Gefahr für Leib, Leben oder Sachen», «neuralgischer Punkt») erfüllt sind,
- der allgemeine verwaltungs- und datenschutzrechtliche Grundsatz der Verhältnismässigkeit gewährleistet ist (§ 8 IDG), und
- eine Reglementspflicht besteht (Art. 10 Abs. 2 DSV).

Zu diesen Punkten hat die zuständige Dienstabteilung zuhanden der Datenschutzstelle zunächst in einem *Bericht* Stellung zu nehmen. Die Datenschutzstelle hat zu den inhaltlichen Anforderungen sog. *Erläuterungen* bereitgestellt und betont, dass sich der Bericht vorab auf die Darlegung dieser drei Punkte zu beschränken hat.

Erst wenn die Voraussetzungen für eine konkrete Videoüberwachung dargelegt werden konnten, ist (allenfalls) ein Reglement zu erstellen[5]. Auch dazu stellt die Datenschutzstelle Hilfsmittel bereit, nämlich ein *Muster-Reglement* sowie entsprechende *Erläuterungen*.

Bestehende Videoüberwachungen müssen bis spätestens 30. September 2012 den neuen gesetzlichen Anforderungen entsprechen und der Datenschutzstelle zur Prüfung unterbreitet werden (Art. 20 DSV). Bei der Datenschutzstelle sind bisher erst vereinzelt Berichte und Reglemente zur Prüfung eingegangen. Dennoch zeigt sich, dass sich die zur Verfügung gestellten Hilfsmittel in der Praxis bewähren. Auch lässt sich bereits sagen, dass die Schwierigkeiten in der Umsetzung der gesetzlichen Bestimmungen bei Art. 9 Abs. 1 DSV liegen, d.h. bei der Beurteilung, ob die Voraussetzungen für eine zulässige Videoüberwachung überhaupt

[1] AS 236.100. [2] Art. 9 und 10 DSV. [3] Zuständig und verantwortlich ist diejenige Dienstabteilung, die eine Videoüberwachung betreibt. [4] Abrufbar unter www.stadt-zuerich.ch/datenschutz, «Informationen für Stadtverwaltung». [5] Art. 10 DSV.



gegeben sind (namentlich die «erhebliche Gefahr für Leib, Leben oder Sachen» an einem «neuralgischen Punkt»). Da die Bestimmung von Art. 9 DSV im Zuge des Gesetzgebungsprozesses verschärft wurde, ist dem gesetzgeberischen Willen (an einer restriktiven Praxis) bei der Umsetzung entsprechend Rechnung zu tragen.

Fragen stellten sich auch im Zusammenhang mit der rechtlichen Qualifikation der Reglemente sowie hinsichtlich Art und Umfang der Publikation. Da es sich bei Videoüberwachungs-Reglementen regelmässig um sog. Allgemeinverfügungen[6] handelt, besteht eine Pflicht zur amtlichen Publikation. Die Dienstabteilungen haben somit ihren Beschluss über den Erlass eines Videoüberwachungs-Reglements unter Bekanntgabe der Beschwerde- bzw. Rekursfrist im Amtsblatt der Stadt Zürich zu veröffentlichen. Die Datenschutzstelle geht davon aus, dass die verantwortlichen Verwaltungsstellen die jeweiligen Reglemente in der Regel auf ihren Websites im Internet veröffentlichen werden.

2 Prostitutionsgewerbeverordnung (PGVO)

Bevor der Stadtrat die Prostitutionsgewerbeverordnung (PGVO) mit Weisung vom 25. Mai 2011 dem Gemeinderat zum Erlass vorlegte[7], unterbreitete er im Januar 2011 diversen Verwaltungsstellen und privaten Institutionen einen ersten Entwurf (vom Dezember 2010) zur Vernehmlassung. Die Datenschutzstelle kritisierte diesen ersten Entwurf im Wesentlichen dahingehend, dass die gesetzlichen Anforderungen der genügenden Bestimmtheit gemäss § 8 Abs. 2 IDG nicht erfüllt seien, da – in Anbetracht der Sensibilität der Informationen – nicht klar genug erkennbar sei, welche Personendaten für welche Zwecke durch die Stadtpolizei bearbeitet werden (dürfen).[8]
In der Folge wurde der Entwurf vom Dezember 2010 unter Mitwirkung der Datenschutzstelle ergänzt und präzisiert, so v.a. hinsichtlich Bewilligungsvoraussetzungen, Kontrollen und Datenbearbeitungen: Aus der überarbeiteten PGVO lässt sich nun erkennen, welche Daten für das Bewilligungsverfahren relevant sind, welche Informationen von den Gesuchstellenden beizubringen sind und welche von der Polizei beschafft werden dürfen. Des Weiteren ist bestimmt, welche Informationsrechte der Polizei bei Kontrollen zustehen und welche Informationspflichten den Salonbetreibern obliegen. Klar umschrieben sind insbesondere auch die zulässigen Zwecke, für welche die Personendaten bearbeitet werden dürfen – aus datenschutzrechtlicher Sicht die zentralste Forderung. So bestimmt Art. 15 E-PGVO, dass die Daten der Prostituierten ausschliesslich zur Administration von Bewilligungen, zur Identifikation von Opfern von Zwangsprostitution und zum Nachweis von Urkundenfälschungen oder Falschlegitimationen bearbeitet werden dürfen. Mit diesen Präzisierungen und Erweiterungen erfüllt die Vorlage des Stadtrats nach Einschätzung der Datenschutzstelle nun die rechtlichen Anforderungen, die sich insbesondere aus dem kantonalen IDG ergeben.

Die aus datenschutzrechtlicher Sicht relevanten Bestimmungen der stadträtlichen Weisung vom 25. Mai 2011 blieben in den parlamentarischen Debatten (inhaltlich) unbestritten. Inzwischen hat der Gemeinderat der Stadt Zürich die Prostitutionsgewerbeverordnung in der Schlussabstimmung vom 7. März 2012 mit grosser Mehrheit angenommen.

3 Polizeiliche Datenbank GAMMA

Der Gemeinderat der Stadt Zürich beschloss am 22. Juni 2011, die Verordnung über die polizeiliche Datenbank GAMMA, die bis zum 31. Dezember 2010 befristet war, nicht zu verlängern.[9] Damit wurde der Stadtpolizei die rechtliche Grundlage entzogen, weiterhin Personendaten zwecks Früherkennung und Verhinderung von Gefährdungen der öffentlichen Sicherheit und Ordnung anlässlich von Sportveranstaltungen in der Datenbank GAMMA zu bearbeiten.[10] Operativ in Betrieb war die Datenbank GAMMA nur während des Kalenderjahrs 2010; seit dem 1. Januar 2011 blieb jegliche Datenbearbeitung auf Anweisung des Polizeivorstehers sistiert.[11] Die Stadtpolizei hat im Berichtsjahr die in GAMMA erfassten Daten gelöscht und sowohl der Geschäftsprüfungskommission des Gemeinderats als auch der Datenschutzstelle die vollständige, ausnahmslose und unwiderrufliche Löschung schriftlich bestätigt.

Trotz der Aufhebung bzw. Nichtverlängerung der Verordnung und der vollständigen Datenlöschung ist das letzte Kapitel in dieser Angelegenheit noch nicht geschrieben. Im Oktober 2011 wurde im Gemeinderat ein Postulat eingereicht, in welchem der Stadtrat gebeten wird, zu prüfen, wie die polizeiliche Datenbank GAMMA wieder eingeführt werden kann.[12]

4 IT-Sicherheitshandbuch

Der Stadtrat hat im Jahr 2005 ein Sicherheitshandbuch in Kraft gesetzt, welches als Standard den IT-Grundschutz in der Stadtverwaltung definiert. Es beinhaltet Anweisungen und Anleitungen zur Etablierung eines umfassenden und kontinuierlichen IT-Sicherheitsprozesses. Zielpublikum sind alle städtischen Mitarbeitenden, die mit Management, Design, Beschaffung, Entwicklung oder Betrieb von Software und IT-Anlagen beauftragt sind. Das Sicherheitshandbuch wird zur Zeit durch die OIZ mit Unterstützung diverser Fachstellen umfassend überarbeitet. Da das Handbuch auch aus Sicht des Datenschutzes von grundlegender Bedeutung ist, hat für die Datenschutzstelle die Mitarbeit bei der Neufassung einen entsprechend hohen Stellenwert eingenommen. Das Anliegen der Datenschutzstelle ist eine möglichst optimale Koordination und Integration datenschutzrechtlicher Vorgaben in die Prozesse und Abläufe der

[6] Allgemeinverfügungen sind generell-konkrete Anordnungen, die Rechte und Pflichten eines geschlossenen oder offenen Kreises nicht individuell bestimmter Adressaten mit Bezug auf einzelne, individuell bestimmte Sachverhalte regeln (H.R. Thalmann, Kommentar zum Zürcher Gemeindegesetz, 3. Auflage 2000, S. 212). [7] GR-Nr. 2011/169. [8] TB 2010, S. 7.

[9] GR-Nr. 2010/418. Über dieses Geschäft hat die Datenschutzstelle in ihren Tätigkeitsberichten regelmässig informiert (TB 2010, S. 5 f.; TB 2009, S. 9 f.; TB 2008, S. 9; TB 2007, S. 10 f.; TB 2006, S. 11 f.). [10] Art. 2 der aufgehobenen Verordnung. [11] Da der Gemeinderat über die beantragte Verlängerung nicht vor Ablauf der Frist (31.12.2010) beschliessen konnte; vgl. TB 2010, S. 5 f. [12] GR-Nr. 2011/375.

Stadtverwaltung. In erster Linie geht es dabei um die optimale Koordination und Integration der mit dem IDG per Oktober 2008 neu eingeführten Vorabkontrolle für datenschutzrechtlich sensible Vorhaben und Projekte. In direktem Zusammenhang mit der Überarbeitung des IT-Sicherheitshandbuchs steht auch die Erarbeitung einer Vorlage für ein Informatiksicherheits- und Datenschutzkonzept (ISDS-Konzept) (vgl. dazu nachfolgend Bericht Nr. 6).

5 Open Government Data (OGD)

Der Stadtrat sieht im Rahmen der Legislaturperiode 2010 bis 2014 mit dem Legislaturschwerpunkt e-Zürich vor, die Stadt Zürich bis im Jahr 2015 europaweit als bevorzugten Standort für ICT-Dienstleistungen und -Infrastrukturen zu positionieren. Aus dem stadträtlichen Legislaturschwerpunkt geht dabei deutlich hervor, dass Datenschutz nicht als blosse gesetzliche Rahmenbedingung, sondern vielmehr als Garant für Vertrauen und somit letztlich als Bedingung für eine breite Akzeptanz und erfolgreiche Umsetzung der e-Zürich-Projekte angesehen wird.

Eine aus den Zielen von e-Zürich abgeleitete strategische Stossrichtung ist, die vorhandene Infrastruktur der Stadt Zürich – worunter insbesondere auch Daten zu zählen sind – breit nutzbar zu machen.[13] Damit ist Open Government Data in Zürich angekommen. Unter diesem Begriff wird die aktive Bereitstellung gesetzlich nicht geschützter Datenbestände der öffentlichen Verwaltung zur freien Einsichtnahme und Wiederverwendung verstanden.[14] Aus dieser Umschreibung ergibt sich, dass all jene Daten(-bestände), die geheim zu halten sind bzw. die Betriebs- und Geschäftsgeheimnisse sowie personenbezogene Daten beinhalten, nicht unter diesen Begriff fallen.

Stellt sich bei Open Government Data somit per definitionem gar kein Datenschutzproblem, da Personendaten gar nicht tangiert sein können? So einfach wird es wohl kaum sein, denn die Beantwortung der Frage, ob Daten einen rechtlich relevanten Personenbezug aufweisen und damit unter den Geltungsbereich der Datenschutzgesetzgebung fallen, kann unter Umständen schwierig sein und setzt auf alle Fälle genaue Sach- und Rechtskenntnisse im jeweiligen Fachbereich voraus. Die Herausforderungen aus datenschutzrechtlicher Optik bestehen somit nicht nur in der Prüfung, ob einer freien Zugänglichkeit von bestimmten Datenbeständen allenfalls Schutz- oder Geheimhaltungsvorschriften entgegen stehen, sondern insbesondere auch in der Klärung der Verantwortung und Zuständigkeit und somit in der Sicherstellung, dass die Prüfung von der richtigen Verwaltungsstelle vorgenommen wird.
Die Datenschutzstelle hat deshalb darauf hingewirkt, dass in der stadträtlichen Open Government Data Policy[15] – der ersten und als solchen immer noch sehr allgemein gehaltenen Umsetzungsmassnahme – ausdrücklich festgehalten wird, dass der Entscheid über die Veröffentlichung eines bestimmten Datensatzes materiell von der in der Sache zuständigen Dienstabteilung zu fällen ist und nicht an andere Dienstabteilungen oder Gremien (bspw. eine Infrastrukturbetreiberin) delegiert werden kann. Die (weitergehende) Konkretisierung der erforderlichen materiellen Prüfung im Einzelfall wird Gegenstand der weiteren Umsetzungsmassnahmen sein müssen. In diesem Sinn dürfte auch das im e-Zürich Legislaturschwerpunkt vom Stadtrat ausdrücklich formulierte Ziel verstanden werden, wonach die Stadt Zürich vertrauenswürdige Datenschutzstandards für alle bereitgestellten Dienstleistungen etablieren will.

6 ISDS-Konzept

Die Datenschutzstelle hatte in den letzjährigen Tätigkeitsberichten[16] darauf hingewiesen, dass die mit dem IDG neu eingeführte Vorabkontrolle[17] nach Möglichkeit in die bestehenden Verwaltungsprozesse einzubinden sei. Nach der zunächst nur formellen Integration der Vorabkontrolle in das Verfahren des städtischen IT-Controllings[18] ist man (insbesondere auch inhaltlich) der Einbindung in bestehende IT-Prozesse inzwischen einen grossen Schritt nähergekommen.

IT-Projekte sind in der Stadtverwaltung nach der Projektführungsmethode HERMES[19] zu führen. HERMES unterteilt ein Projekt in verschiedene Projektphasen[20] und beschreibt die pro Projektphase jeweils zu erfüllenden Aufgaben und Ergebnisse. Angaben zur Erhaltung und Verbesserung des Datenschutzes und der Informationssicherheit sind dabei in einem sog. Informationssicherheit- und Datenschutz-Konzept (kurz: ISDS-Konzept) festzuhalten.

Im Berichtsjahr hat die Datenschutzstelle nun in Zusammenarbeit mit OIZ und IT-Controlling eine städtische ISDS-Konzeptvorlage samt beschreibender Wegleitung erarbeitet, welche auf den Vorgaben und Methoden von HERMES basiert, aber spezifisch auf die Gegebenheiten und Bedürfnisse der Stadtverwaltung ausgerichtet ist. Im Wesentlichen handelt es sich dabei um Vorlagen zu Systembeschrieb, Datenbearbeitungsprozessen, Risikoanalysen sowie Sicherheitsmassnahmen (inkl. Beschrieb von Restrisiken). Die Konzeptvorlage ermöglicht es den Projektverantwortlichen, die massgebenden Projektangaben und Informationen zum richtigen Zeitpunkt, in der gewünschten Form und in einem einfachen und koordinierten Verfahren beiden beteiligten Prüfinstanzen (der Datenschutzstelle zur Durchführung der Vorabkontrolle, der OIZ zur Prüfung der Informationssicherheit) bereitzustellen.

Für die datenschutzrechtliche Vorabkontrolle sind regelmässig spezialgesetzliche Rechtsgrundlagen aus den jeweiligen

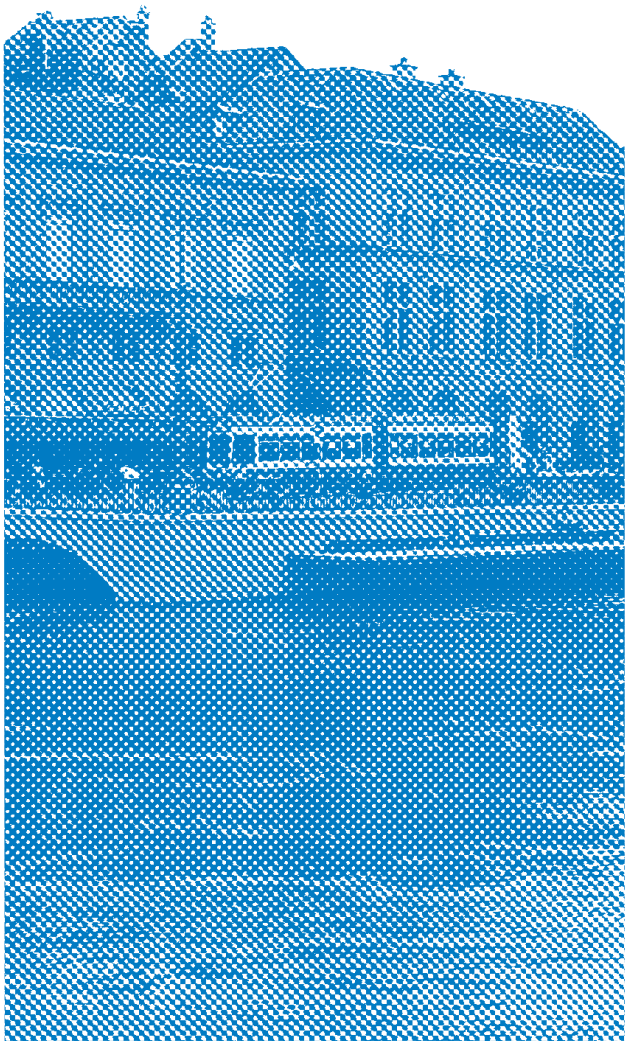
[13] StRB 948/2011 vom 24. August 2011. [14] Open Government Data Manifest für die Schweiz, www.opendata.ch. [15] Diese Policy des Stadtrats liegt zur Zeit als Entwurf vor.

[16] TB 2009, S. 3 f.; TB 2008, S. 4. [17] § 10 IDG: «Das öffentliche Organ unterbreitet 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.» [18] TB 2008, S. 4. [19] www.hermes.admin.ch. [20] Initialisierung, Voranalyse, Evaluation, Implementierung, Einführung und Abschluss.

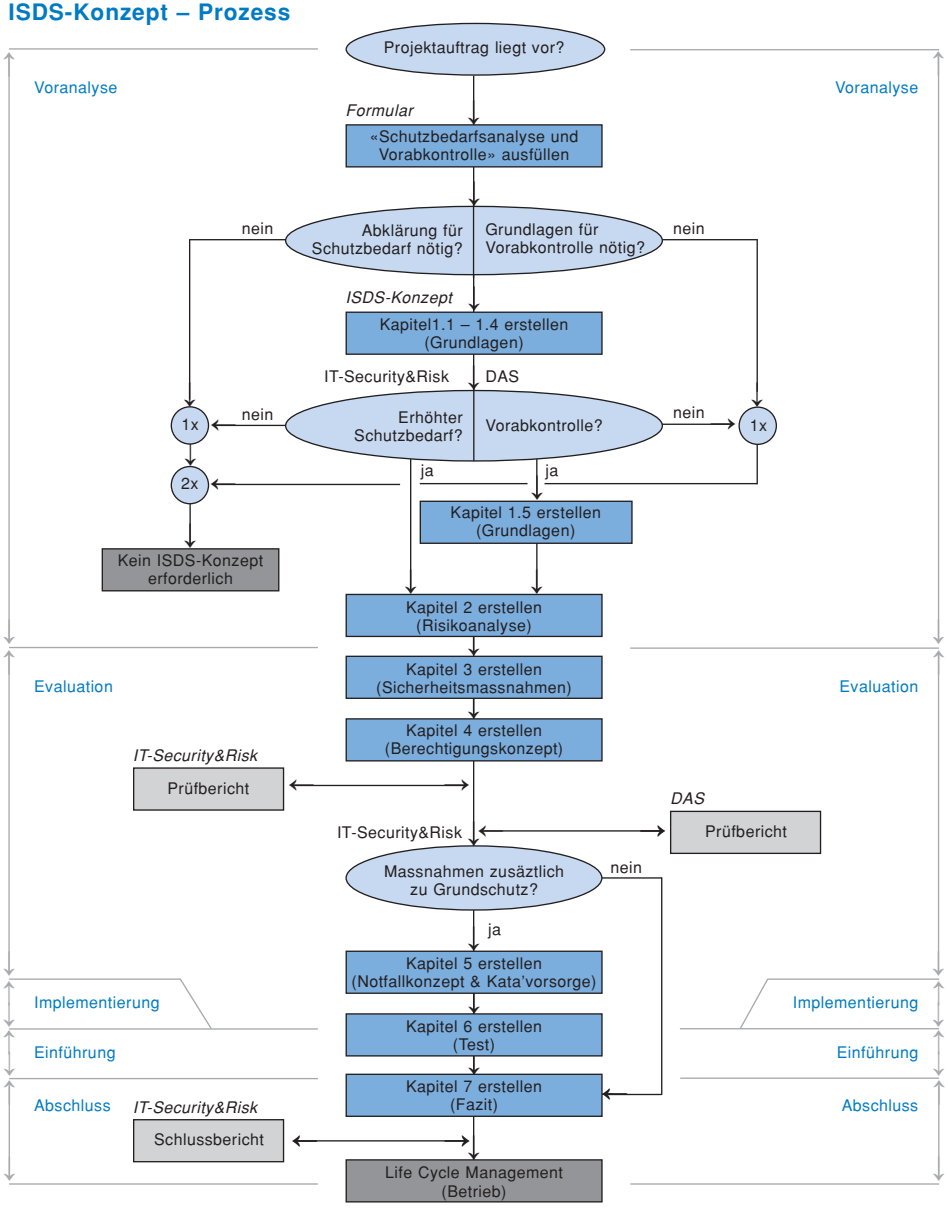
Fachgebieten von Relevanz. Die verantwortlichen Verwaltungsstellen sind deshalb gesetzlich verpflichtet, der Datenschutzstelle eine Darstellung der Rechtslage einzureichen.[21] Um eine Fokussierung auf die wesentlichen (datenschutz-)rechtlichen Fragestellungen erreichen und damit auch diesbezüglich unnötigen Aufwand vermeiden zu können, prüft die Datenschutzstelle diese Bringschuld jeweils vorgängig und konkretisiert sie gegebenen falls mittels direktem Auftrag an den zuständigen Rechtsdienst. Dank dem ISDS-Konzept können auch dem jeweiligen Rechtsdienst die zu diesem Zeitpunkt vorhandenen Projektinformationen in aufbereiteter und systematischer Form zur Verfügung gestellt werden.

Für Projektverantwortliche und Prüfinstanzen schaffen die gemeinsame ISDS-Konzeptvorlage und die Koordination der beiden Prüfverfahren grosse Vorteile. Mit der Klärung des Informationsbedürfnisses in inhaltlicher, formeller und zeitlicher Hinsicht werden nicht nur Doppelspurigkeiten bei der Erarbeitung von Projektinformationen und -dokumentationen vermieden (was für alle Beteiligten viel Aufwand und Zeit spart), sondern kann auch eine Erhöhung der Prüfungsqualität seitens Datenschutzstelle und OIZ erreicht werden. Erste Erfahrungen zeigen denn auch, dass die neue ISDS-Konzeptvorlage sowie die damit verbundenen Prozesse von den Projektbeteiligten positiv aufgenommen werden.

[21] § 24 Abs. 2 lit. b IDV.



ISDS-Konzept – Prozess



7 Gebäudedatenpool (GDP)

Zahlreiche Dienstabteilungen der Stadtverwaltung sind für die Erfüllung ihrer gesetzlichen Aufgaben auf Grundstück-, Gebäude- und Wohnungsdaten angewiesen. Bisher haben die Dienstabteilungen die einzelnen Daten entweder über einen Datenpool oder bei der jeweiligen, für die Bewirtschaftung der Daten zuständigen Dienstabteilung bezogen. Dies hat in der Praxis technisch und organisatorisch zu komplizierten und wenig transparenten Austauschverhältnissen geführt. Im Auftrag der Dienstabteilungen Geomatik + Vermessung (GeoZ), Amt für Baubewilligungen (AfB), Amt für Städtebau (AfS) und Statistik Stadt Zürich (SSZ) wurde nun durch die OIZ ein Gebäudedatenpool (GDP) aufgebaut, mit welchem ein neuer Ansatz verfolgt wird[22]: Den Dienstabteilungen sollen zur Erfüllung ihrer Aufgaben nicht mehr (nur) einzelne Daten, sondern auf ihre Bedürfnisse angepasste Services mit unterschiedlichen «Datenpaketen» zur Verfügung gestellt werden. Aktuell sind am technisch und konzeptionell neu ausgerichteten Gebäudedatenpool die erwähnten Dienstabteilungen – sowohl in der Rolle als Datenlieferanten als auch als Service-Nutzer – beteiligt. Weitere Dienstabteilungen sollen in absehbarer Zukunft an den Gebäudedatenpool angebunden werden, was auch einen Weiterausbau des Service-Angebots zur Folge haben wird.

Die Datenschutzstelle hat gestützt auf eine von ihr bei den beteiligten Dienstabteilungen durchgeführten Umfrage festgestellt, dass die Verantwortlichkeiten in Bezug auf die unterschiedlichen Rollen der Dienstabteilungen (als Datenlieferanten, Service-Nutzer oder als Systembetreiber) nicht geklärt wurden und eine rechtliche Überprüfung der Nutzungsvoraussetzungen der GDP-Services bisher nicht vorgenommen worden ist. Die Datenschutzstelle verlangte, dass diese Prüfung nachgeholt wird und hat – unter Einbezug der zuständigen Rechtsdienste – das Prüfverfahren festgelegt und ein entsprechendes Prüfungsschema ausgearbeitet. Dieses basiert in erster Linie auf der Geoinformationsgesetzgebung des Bundes und des Kantons, da es sich bei den im Gebäudedatenpool bearbeiteten Daten zu einem grossen Teil um raumbezogene Daten handelt (bspw. Angaben wie Bodenbedeckungsart, Flächenmass, Gebäudeart, Gebäudenummer, Wohnanteil, Zonenstatus, Zonenart). Die Geoinformationsgesetzgebung geht vom Grundsatz der freien Zugänglichkeit solcher Daten aus[23] und verlangt von den Behörden, dass sie sich untereinander einfachen und direkten Zugang zu den Daten gewähren[24]. Allerdings gilt dies nicht absolut: Bei gewissen Daten muss der Zugang verweigert werden, wenn die Behörde ein öffentliches Interesse nicht nachweisen kann oder allfällige Sicherheitsüberlegungen einer Nutzung entgegenstehen.[25]

[22] Der neue Gebäudedatenpool basiert auf der mit der IT-Strategie der Stadt Zürich festgelegten sog. Service-orientierten Architektur (SOA). [23] Art. 10 GeoIG; SR 510.62.
[24] Art. 14 GeoIG; § 13 E-KGeoIG; KR-Nr. 4703/2010. [25] Art. 38 GeoIV; SR 510.620.

Vor diesem Hintergrund haben die Dienstabteilungen – in der Rolle als Datenlieferanten – mit Hilfe des Prüfungsschemas in einem ersten Schritt eine der Geoinformationsgesetzgebung entsprechende Klassifizierung sämtlicher im Gebäudedatenpool zur Verfügung gestellten Daten mit Angabe der Zugangsberechtigungsstufe[26] und allfälliger spezieller Nutzungsbestimmungen vorzunehmen. Bei Daten, welche nicht unter den Geltungsbereich der Geoinformationsgesetzgebung fallen, müssen weitere Angaben, bspw. zu den massgebenden Rechtsgrundlagen, gemacht werden. Mit diesem Vorgehen können für sämtliche im Gebäudedatenpool bereitgestellten Daten die Nutzungsvoraussetzungen geklärt werden. Gestützt auf diese Grundlageninformationen, welche von den Datenlieferanten für die einzelnen Daten nur einmal erarbeitet werden müssen, können anschliessend mit wenig Aufwand für jeden einzelnen Service die Nutzungsvoraussetzungen – und zwar unabhängig von einem konkreten Datennutzer – bestimmt werden: Die OIZ als Betreiberin kann dadurch Services, welche auf Grund der von den Datenlieferanten mittels Prüfungsschema gemachten Angaben ohne spezielle Voraussetzungen genutzt werden dürfen, den Dienstabteilungen ohne weitere Abklärungen zur Verfügung stellen. Nur bei Services, welche speziellen Nutzungsvoraussetzungen unterliegen, ist dann in einem weiteren Schritt jeweils zu prüfen, ob die einzelnen Datennutzer die entsprechenden Voraussetzungen für die gewünschte Service-Nutzung erfüllen. Für die materielle Kontrolle dieser Prüfungen werden die jeweilig zuständigen Datenlieferanten verantwortlich sein. Das Prüfungsschema trägt damit wesentlich zu einer effizienten Steuerung eines rechtskonformen GDP-Betriebes bei.

Die Dienstabteilungen sind zur Zeit daran, ihre im Gebäudedatenpool bereitgestellten Daten anhand des Prüfungsschemas zu klassifizieren und die einzelnen Nutzungsverhältnisse zu überprüfen. Diese Abklärungen werden zeigen, ob und wo das Service-Angebot allenfalls angepasst werden muss.

8 Zugangskontrolle K&A

Das Sozialdepartement der Stadt Zürich betreibt vier Kontakt- und Anlaufstellen (K&A) für Drogen konsumierende Personen[27]. Zugang zu den K&A haben grundsätzlich nur Personen mit Wohnsitz in der Stadt Zürich. Sowohl diese Zutrittsvoraussetzung als auch die Durchsetzung allfälliger Hausverbote[28] erfordern entsprechende Eingangskontrollen, welche durch Mitarbeitende der sip züri (Sicherheit Intervention Prävention) wahrgenommen werden.

Bis anhin hatten die Klienten am Eingang einer K&A entweder eine ID und ein offizielles Dokument mit Wohnsitzangabe oder eine von den K&A ausgestellte Zutrittskarte vorzuweisen; die sip-Mitarbei-

[26] Art. 21 GeoIV. [27] Die Datenschutzstelle berichtete in einer anderen Angelegenheit bereits über diese Institutionen (TB 2009, S. 14 f.; Personenkontrollen in und um K&A).
[28] Solche Hausverbote werden bspw. bei Verstössen gegen die Hausordnung, bei Hausfriedensbruch oder bei Gewalt gegen andere Klienten oder Mitarbeitende ausgesprochen.

tenden prüften dann jeweils anhand von tagesaktuellen Listen, ob gegen die betreffende Person allenfalls ein Hausverbot vorliegt. Dieses «papierlastige» Zutrittsprozedere sollte durch eine elektronische Variante ergänzt werden. Die Datenschutzstelle wurde darüber Ende Dezember 2010 in einer frühen Phase des IT-Projekts orientiert und hat das Projekt bis zur Realisierung begleitet.

Neu steht den Klienten von K&A mit Wohnsitz in der Stadt Zürich die Möglichkeit offen, einem sog. Member Club beizutreten. Dieser basiert darauf, dass in einer Datensammlung persönliche Angaben hinterlegt werden, welche die Identifizierung eines Mitgliedes erlauben (so v.a. aufgrund des hinterlegten Fotos). Für die Eingangskontrolle kann somit entweder die Membercard gezeigt oder – falls diese vergessen oder verloren gegangen ist – der (Gassen-)Name genannt werden.

Die für die Mitgliedschaft in einer Datensammlung hinterlegten persönlichen Angaben erlauben aber nicht nur den Mitgliedern einen «papierlosen» Eintritt, sondern vereinfachen und vereinheitlichen auch die Überprüfung der Zugangsberechtigung für die sip-Mitarbeitenden. Diese können mit mobilen Geräten auch überprüfen, ob gegen eine Einlass begehrende Person zum aktuellen Zeitpunkt ein Hausverbot vorliegt oder nicht, da unabhängig von einer Mitgliedschaft künftig auch die Hausverbote elektronisch erfasst werden.

Im Rahmen der Umsetzung des Projekts galt es angesichts des sensiblen Kontextes der Datenbearbeitung (Drogenabhängigkeit) in verschiedener Hinsicht sicherzustellen, dass den Anliegen des Datenschutzes und der Datensicherheit ausreichend Rechnung getragen wird. Beispielsweise galt es darauf zu achten, dass die Mitgliederkarten so ausgestaltet werden, dass sie keine Rückschlüsse auf den «Club» zulassen. Dies führte dazu, dass die Mitgliederkarten schliesslich neutral gehalten und nur mit einem Barcode versehen wurden, welcher mit den mobilen Geräten eingescannt werden kann. Da durch das Einscannen des Barcodes die für die Identifizierung notwendigen Personendaten auf den mobilen Geräten abgerufen werden können, haben die mobilen Geräte verschiedene Sicherheitsanforderungen zu erfüllen (verschlüsselter Zugriff auf die Web-Anwendung, Login, Löschung der Daten bei mehreren fehlerhaften Login-Versuchen). Schliesslich hat die Datenschutzstelle auch darauf hingewiesen, dass angesichts der elektronischen Lösung auf die bisherigen ausgedruckten, nun redundanten Listen mit den Hausverboten verzichtet werden kann. Das neue elektronische Zutrittsprozedere wurde Mitte 2011 in Betrieb genommen und erfüllt nach Beurteilung der Datenschutzstelle sämtliche datenschutzrechtlichen Anforderungen.

9 Anlaufstelle für Vermieter

Die Sozialen Dienste der Stadt Zürich bieten seit November 2011 eine Anlaufstelle für Vermieter an. Vermieterinnen und Vermieter können sich bei Schwierigkeiten in einem Mietverhältnis – bspw. bei Mietrückständen, wiederholten Verletzungen der Hausordnung oder schweren Nachbarschaftskonflikten – an die Anlaufstelle wenden. Die frühzeitige Beratung und Vermittlung der Anlaufstelle soll dazu beitragen, Kündigungen und Ausweisungen zu vermeiden.[29]

Die Dienstleistungen, welche die Anlaufstelle anbietet, bringen regelmässig die Bearbeitung von personenbezogenen Informationen mit sich: So beinhalten die der Anlaufstelle im Hinblick auf eine Beratung geschilderten Sachverhalte nebst Namen immer auch Angaben über das beanstandete Fehlverhalten bestimmter Mieterinnen oder Mieter. Bei den der Anlaufstelle mitgeteilten Informationen handelt es sich somit regelmässig um sensible Daten im Sinne der Datenschutzgesetzgebung. Zudem wird es für eine erfolgreiche Beratung und insbesondere eine Vermittlung zwischen den Parteien oft auch unerlässlich sein, dass diese (und allenfalls weitere sensible) Informationen nicht nur von der Vermieterschaft an die Verwaltung fliessen, sondern auch (wieder) in umgekehrter Richtung zurück, nämlich von der Verwaltung an die (private) Vermieterschaft.

Die Sozialen Dienste haben sich für die Klärung der diversen datenschutzrechtlichen Fragestellungen an die Datenschutzstelle gewandt. Im Wesentlichen ging es dabei um folgende Themen:

- Zulässigkeit eines Beratungs- und Dienstleistungsangebots, welches die Bekanntgabe sensibler Personendaten von (privaten) Mietern mittels Meldung durch (private) Vermieter an die Verwaltung mit sich bringt;
- Qualifikation der Dienstleistungen der Anlaufstelle für betroffene Mieterinnen und Mieter (Pflicht- oder freiwilliges Angebot?);
- Zulässigkeit, Voraussetzungen und Inhalt von Auskünften an die (private) Vermieter- bzw. Mieterschaft. D.h. Klärung des Verhältnisses zwischen Schweigepflicht gemäss kantonalem Sozialhilfegesetz[30] und Informationsrückfluss von der Verwaltung an die Vermieterschaft bzw. Zusammenarbeit zwischen Verwaltung und Vermieter-/Mieterschaft.

Das kantonale Sozialhilfegesetz verlangt von den Gemeinden, dass mit vorbeugenden Massnahmen Notsituationen abgewendet werden.[31] Da Kündigungen und Ausweisungen aus einer Wohnung zu Notsituationen im Sinne der Sozialhilfegesetzgebung führen (können), muss die Stadt Zürich nach Auffassung der Datenschutzstelle berechtigt sein, die zur Verhinderung solcher Notsituationen geeigne-

[29] Weitere Informationen auf der Website des Sozialdepartements der Stadt Zürich unter Register «Beratungsangebot». Auch Mieterinnen und Mietern können die Dienstleistungen der Anlaufstelle in Anspruch nehmen. [30] § 47 SHG; in Kraft seit dem 1. Januar 2012.
[31] § 1 Abs. 2 und § 4 SHG.

ten Dienstleistungen anzubieten und die hierfür erforderlichen Informationen entgegen zu nehmen.[32]

Ist der von einer Meldung betroffene Mieter nicht bereits Klient der Sozialen Dienste und will er das Angebot der Anlaufstelle nicht in Anspruch nehmen, ist dies seitens der Verwaltung zu respektieren.[33] Eine Datenbearbeitung bzw. mieterbezogene Auskünfte an die Vermieterschaft dürfen in diesem Falle nicht erfolgen. Betrifft die Meldung dagegen einen Mieter, der bereits Klient der Sozialen Dienste ist, dürfen die Informationen zur verwaltungsinternen Prüfung allfälliger Massnahmen (wie bspw. Direktzahlungen der Mietzinse an die Vermieterschaft) verwendet werden.

Wie alle Vermittlungs- und Beratungsdienstleistungen muss auch das Angebot der Anlaufstelle auf Vertrauen und Einverständnis der Beteiligten basieren. In der Praxis wird deshalb mittels Vollmachtserklärungen sichergestellt, dass sich die Dienstleistungen der Anlaufstelle stets auf die Zustimmung sowohl der Mieter- wie auch der Vermieterschaft abstützen lassen. Gleichzeitig kann damit gewährleistet werden, dass allfällige Informationserteilungen der Verwaltung nicht gegen die erwähnte gesetzliche Schweigepflicht verstossen.

10 Auskunftspflicht gegenüber Polizei

Dürfen städtische Mitarbeitende der Polizei gegenüber Auskunft erteilen? Oder sind sie sogar dazu verpflichtet? Welche Anforderungen stellt das Datenschutzrecht an eine Auskunftserteilung und wie lässt sich eine Anfrage der Polizei um telefonische oder mündliche Auskunft mit dem Amts- oder Berufsgeheimnis vereinbaren, welches die Angefragten zu beachten haben und dessen Verletzung unter Strafe steht? Mit solchen und ähnlichen Fragen richteten sich Mitarbeitende der Stadtverwaltung auch im Berichtsjahr an die Datenschutzstelle. So einfach diese Fragestellungen erscheinen, so schwierig ist deren Beantwortung, insbesondere wenn eine möglichst allgemeine Antwort gewünscht wird, die für eine Vielzahl von Anwendungsfällen Geltung haben soll. Der Grund für diese Schwierigkeiten ist auf folgende Besonderheiten im Polizeirecht zurückzuführen:

Das polizeiliche Handeln wird üblicherweise in zwei Hauptkategorien unterteilt: einerseits in das gerichts- bzw. kriminalpolizeiliche, andererseits in das ordnungs- bzw. sicherheitspolizeiliche Handeln. Die jeweiligen polizeilichen Tätigkeiten basieren auf unterschiedlichen Rechtsgrundlagen: Für die kriminalpolizeiliche Tätigkeit bzw. die Strafverfolgung ist in erster Linie die auf den 1. Januar 2011 in Kraft getretene gesamtschweizerische Strafprozessordnung (StPO) massgebend, für die sicherheitspolizeiliche Tätigkeit das jeweilige kantonale Polizeigesetz (PolG). Welches Recht Anwendung findet, kann unter Umständen schwierig zu beantworten sein, da Massnahmen der Strafverfolgung gleichzeitig auch der Gefahrenabwehr dienen können und umgekehrt. Für zahlreiche polizeiliche Handlungen lässt sich somit eine klare Trennung nach kriminal- oder sicherheitspolizeilicher Tätigkeit, also nach dem Anwendungsbereich von StPO bzw. PolG, nur schwer oder gar nicht vornehmen.[34]

Erschwerend kommt hinzu, dass die einzelnen Rechtsgrundlagen die Frage nach Recht oder Pflicht zur Auskunft oft nicht mit der erwünschten Klarheit regeln. Im Rahmen der Strafverfolgung sind Auskunftsrechte und -pflichten von Verwaltungsstellen gegenüber der Polizei in der StPO nicht explizit geregelt, sondern fallen unter die Bestimmungen der sog. Rechtshilfe[35]. Eine Verpflichtung von Verwaltungsstellen zur Rechtshilfe und somit eine Verpflichtung zur Auskunftserteilung gegenüber der Polizei besteht danach erst dann, wenn das Verfahren unter der Führung und der Weisung der Staatsanwaltschaft steht (d.h. in der Regel mit Eröffnung eines Strafverfahrens)[36]. Solange ein Ermittlungsverfahren noch in der selbständigen Zuständigkeit der Polizei steht, statuiert die StPO für Verwaltungsstellen keine Auskunftspflichten. Das PolG des Kantons Zürich sieht im Gegensatz zur StPO für die sicherheitspolizeiliche Tätigkeit demgegenüber wieder explizit eine Auskunftspflicht der Verwaltungsstellen gegenüber der Polizei vor.[37]

Dies kann im Ergebnis dazu führen, dass zu Beginn einer polizeilichen Ermittlung eine Auskunftspflicht der Verwaltung besteht (da das PolG massgebende Rechtsgrundlage ist), dass aber im Verlaufe der Ermittlung (da nun aufgrund der mittlerweilen vorliegenden Erkenntnisse die StPO zur Anwendung kommt) diese Auskunftspflicht nicht mehr bzw. erst wieder besteht, wenn das Verfahren unter der Leitung der Staatsanwaltschaft steht.[38] Aufgrund dieser komplexen rechtlichen Ausgangslage ist verständlich, dass angefragte Verwaltungsstellen kaum in der Lage sein werden, zu beurteilen, ob in einer konkreten Situation ein Auskunftsrecht oder eine Auskunftspflicht besteht, ist diese Beurteilung doch selbst für Polizistinnen und Polizisten äusserst schwierig. Die Datenschutzstelle empfiehlt deshalb, Auskünfte, die sensible Personendaten enthalten oder einer Geheimhaltungspflicht (Amts- oder Berufsgeheimnis) unterstehen können, nur auf schriftliche Anfrage der Polizei hin zu erteilen. Die in einer solchen polizeilichen Anfrage anzugebende Rechtsgrundlage erlaubt es, dass das Vorliegen einer bestehenden Auskunftspflicht bzw. eines Auskunftsrechts vorab mit der erforderlichen Sorgfalt geprüft werden kann. Letztlich muss somit jede polizeiliche Anfrage einer Einzelfallprüfung unterzogen werden; eine Pauschalantwort ist nicht möglich.

[32] Hinsichtlich Wichtigkeit von präventivem Handeln bzw. Früherkennung vgl. Tages-Anzeiger vom 2. November 2011 (Interview mit Stadtrat Waser) sowie NZZ am Sonntag, 18. März 2012.
[33] §§ 16 und 25 SHV.
[34] Daniel Kettiger, Schnittstellenfragen der Schweizerischen Strafprozessordnung, Rz 7, in: Jusletter 13. Februar 2012.
[35] Art. 43 ff. StPO.
[36] Art. 43 Abs. 2 StPO.
[37] § 54 Abs. 2 PolG.
[38] Nebst der StPO und den kantonalen PolG besteht eine Vielzahl weiterer polizeilicher Rechtsgrundlagen, welche für die Frage, ob ein Recht oder eine Pflicht zur Auskunftserteilung an die Polizei besteht, ausschlaggebend sind.

11 Meldeverfahren Prostituierte

Im Sommer 2011 berichteten verschiedene Medien, dass die Stadtpolizei noch vor Inkrafttreten der neuen Prostitutionsgewerbeverordnung (PGVO)[39] ein neues Prüfungsverfahren für Prostituierte eingeführt habe, mit welchem die Prostituierten «auf Herz und Nieren» geprüft würden.[40] Da eine derartige Überprüfung der Prostituierten durch die Stadtpolizei im damaligen Entwurf der PGVO nicht vorgesehen war, untersuchte die Datenschutzstelle dieses Prüfungsverfahren näher.

Selbständigerwerbende aus den EU-25/EFTA-Staaten können in der Schweiz ohne Bewilligung, aber mit obligatorischer Meldung, während bis zu 90 Arbeitstagen pro Kalenderjahr arbeiten. Zuständig für dieses Meldeverfahren im Kanton Zürich ist das kantonale Amt für Wirtschaft und Arbeit (AWA).

Im Bereich der Stassenprostitution wird die Selbständigkeit angesichts der Gefahr von Scheinselbständigkeit bzw. Zwangsprostitution – anders als bei den übrigen Dienstleistungserbringenden – systematisch im Voraus geprüft. Da die Abklärung der Selbständigkeit spezifische Kenntnisse des Prostitutionsgewerbes und Sexmilieus voraussetzt, hat das AWA die Stadtpolizei mit dieser Überprüfung beauftragt. Seit Sommer 2011 führt die Stadtpolizei im Rahmen eines Pilotprojekts mit allen Prostituierten, die auf dem Strassenstrich der Stadt Zürich arbeiten wollen, ein persönliches Gespräch, anhand dessen Selbständigkeit und Selbstbestimmung der jeweiligen Gesuchstellerinnen beurteilt wird. Im Anschluss gibt die Stadtpolizei dem AWA jeweils eine entsprechende Empfehlung ab.

Dieser Auftrag basiert auf einer Vereinbarung zwischen der Volksdirektion des Kantons Zürich und dem Polizeidepartement der Stadt Zürich. Aus datenschutzrechtlicher Sicht ist gegen eine derartige Auftragserteilung des AWA und der damit verbundenen Datenbearbeitung durch die Stadtpolizei grundsätzlich nichts einzuwenden. Kritisiert werden musste jedoch, dass die Vereinbarung nicht allen Anforderungen entspricht, welche IDG und IDV an eine Datenbearbeitung im Auftrag stellen[41]. Die Datenschutzstelle[42] hat deshalb die Vertragsparteien auf notwendige Ergänzungen aufmerksam gemacht (insbesondere betreffend einer Regelung, wonach die Stadtpolizei die erhobenen Daten ausschliesslich im Rahmen ihres Auftrags bearbeiten darf, sämtliche Daten dem AWA weiterleiten muss und nicht berechtigt ist, die Daten zu eigenen polizeilichen Zwecken weiter zu verwenden).

Der Datenschutzbeauftragte hat die Stadtpolizei und das Polizeidepartement darüber hinaus darauf hingewiesen, dass die Vereinbarung mit dem AWA aus städtischer Optik auch vor dem Hintergrund der neu geschaffenen PGVO zu beurteilen ist. Diese definiert die zulässigen Datenbearbeitungen der Stadtpolizei im Bereich der Prostitution in einem abschliessenden und damit begrenzenden Sinne. Für das AWA erhebt die Stadtpolizei weitergehende und detailliertere Informationen, als sie es für den Vollzug der PGVO benötigt. Für letzteres genügen grundsätzlich diejenigen Informationen, die für die Administration der Bewilligungen erforderlich sind. Eine Datenerhebung, wie sie die Stadtpolizei im Auftrag des AWA durchführt, ist demgegenüber in der PGVO gerade nicht vorgesehen. Eine derartige Konstellation (über die eigene Kompetenz gemäss PGVO hinausgehende Datenbearbeitung im Auftrag des AWA) beinhaltet Konfliktpotential, so dass von den hierfür verantwortlichen Organen die Frage zu klären sein wird, ob das Prüfungsverfahren durch die Stadtpolizei im Auftrag des AWA zukünftig unter dem Geltungsbereich der neuen PGVO noch opportun und zulässig ist.

12 Publikation über ehemalige Ratsmitglieder

Im letztjährigen Tätigkeitsbericht thematisierte die Datenschutzstelle schwerpunktmässig die Veröffentlichung von Personendaten im Internet.[43] Auch im Berichtsjahr war diese Thematik Gegenstand diverser Anfragen und Abklärungen. Eine davon betraf den Gemeinderat quasi in eigener Sache: Zur Frage stand, inwieweit ein Ratsmitglied nach Ausscheiden aus dem Stadtparlament verlangen darf, dass seine Angaben zur Person auf der Website des Gemeinderats im Verzeichnis der Mitglieder[44] (nicht aber in den Vorstössen und Protokollen) zu löschen seien. Nach Ansicht der Datenschutzstelle handelt es sich bei der Information, wer Mitglied des Gemeinderats ist bzw. war, um eine Information von allgemeinem Interesse im Sinne von §14 IDG. Die Stadt Zürich ist somit grundsätzlich verpflichtet, diese Informationen von Amtes wegen zur Verfügung zu stellen. Wie bei jeder Bekanntgabe von Personendaten ist aber eine Interessensabwägung vorzunehmen. Zur Diskussion stehen Informationen, die in Zusammenhang mit der Ausübung eines öffentlichen Amts stehen, somit aus einer eigentlich öffentlichen Sphäre und nicht aus der Geheim- oder Privatsphäre einer Person stammen. Schon dadurch ist der Eingriff in die Persönlichkeitssphäre, welcher mit der Publikation des Mitgliederverzeichnisses im Internet verbunden ist, als gering zu qualifizieren. Dem sind die öffentlichen Interessen nach Transparenz, Nachvollzieh- und Kontrollierbarkeit in Bezug auf die legislative Gewalt gegenüber zu stellen – Interessen, die sich aufgrund ihrer institutionellen Relevanz nicht auf die Aktivzeit der jeweiligen Parlamentarier beschränken können. Die öffentlichen Interessen überwiegen nach Ansicht der Datenschutzstelle klar die privaten Interessen, so dass ein Anspruch der Ratsmitglieder auf umfassende Löschung aller personenbezogenen Daten nach Ausscheiden aus dem Gemeinderat nicht besteht. Auch beurteilte die Datenschutzstelle die Informationen, die über ehemalige

[39] Vgl. dazu vorne Bericht Nr. 2. [40] So bspw. die Berichterstattung in der Neuen Zürcher Zeitung vom 28. Juli 2011. [41] § 6 IDG, § 25 IDV. [42] Da mit dem AWA auch eine kantonale Verwaltungsstelle involviert ist, hat die städtische Datenschutzstelle auch den kantonalen Datenschutzbeauftragten beigezogen.

[43] TB 2010, S. 2 ff. [44] Zu finden unter www.gemeinderat-zuerich.ch/mitglieder.aspx.

Ratsmitglieder veröffentlicht bleiben sollen, als verhältnismässig. Die Publikation von Name, Amtsdauer, Parteizugehörigkeit, eingereichten Vorstössen und Mitgliedschaften in Kommissionen umfasst nur diejenigen Informationen, die erforderlich und geeignet sind, das öffentliche Informationsbedürfnis zu erfüllen. Damit wird auf die privaten Interessen bzw. die informationelle Privatheit der ehemaligen Ratsmitglieder weitestgehend Rücksicht genommen.

13 Angaben über Patientinnen und Patienten durch die Einwohnerkontrolle

Klärt eine medizinische Klinik bei der Einwohnerkontrolle einer Gemeinde Personalien von Patientinnen und Patienten[45] unter Hinweis auf ein aktuelles Forschungsvorhaben näher ab, offenbart sie damit Patientengeheimnisse. Anhand der Angaben zum Forschungsprojekt, allenfalls bereits schon aufgrund des Namens des Gesuchstellers, lässt sich auf bestimmte gesundheitliche Probleme der Betroffenen schliessen (bspw. Auskunftsgesuche der Onkologie bzw. Psychiatrischen Abteilung über Einwohnerinnen und Einwohner im Rahmen einer Krebs- oder Psychiatrieforschung). Die Datenschutzstelle prüfte aus Anlass eines konkreten Forschungsvorhabens die Voraussetzungen für die Zulässigkeit solcher Abklärungen von Patienten-Personalien.
Auf Bundesebene besteht für die Offenbarung von Patientengeheimnissen bei Forschungen im Bereich der Medizin und des Gesundheitswesens eine abschliessende Regelung (Art. 321bis Abs. 2 und 3 StGB). So dürfen Berufs- bzw. Patientengeheimnisse bei solchen Forschungsvorhaben nur offenbart werden, wenn eine Sachverständigenkommission bzw. Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung[46] dies bewilligt und die betroffenen Patientinnen und Patienten dies nach Aufklärung über ihre Rechte nicht ausdrücklich untersagt haben (Veto- oder Widerspruchsrecht). Liegt keine Bewilligung der Expertenkommission vor, dürfen Patientendaten nur dann bekannt gegeben werden, wenn die betroffenen Patientinnen und Patienten selber ihre Einwilligung zur Datenweitergabe erteilt haben.

Gemäss Auskunft der Gesundheitsdirektion des Kantons Zürich sowie dem Sekretariat der Expertenkommission des Bundes[47] ist die vorliegend zu beurteilende Abklärung von Patienten-Personalien bei einer Einwohnerkontrolle nicht durch das Vorliegen einer sog. «generellen Bewilligung» der Expertenkommission abgedeckt. Eine solche Bewilligung ermächtige lediglich das mit betriebsinternen Forschungstätigkeiten betraute Personal, die (für interne Forschungsprojekte) relevanten Informationen spitalinternen Datenbanken, Papierdaten und Krankengeschichten zu entnehmen. Die Expertenkommission stelle für Abklärungen bei den Einwohnerkontrollen auch keine Sonderbewilligungen aus. Auch die kantonalen Ethikkommissionen könnten für derartige Abklärungen keine eigentlichen Entbindungen vom Berufsgeheimnis aussprechen[48].
Abklärungen bei den Einwohnerkontrollen zu Personalien von Patientinnen und Patienten im Rahmen von Forschungsprojekten sind damit nach geltender Rechtslage weder gestützt auf eine generelle Bewilligung der Expertenkommission, noch auf die Bewilligung einer kantonalen Ethikkommission, sondern nur mit Einwilligung der betroffenen Patientinnen und Patienten zulässig.

14 Datenschutz im Rahmen der Integrationsförderung

Die Stadt Zürich finanziert im Rahmen der Integrationsförderung mit sog. Sprachförderkrediten Deutschkurse für fremdsprachige Erwachsene mit. Solche von der Stadt mitfinanzierten Deutschkurse werden von externen Sprachkursanbietern angeboten, welche – zuhanden der Integrationsförderung der Stadt Zürich (IF) – durch ihre Kursleitenden Daten über die Kursteilnehmenden erheben lassen müssen. Diese Datenerhebungen durch private Sprachkursanbieter und deren Datenweiterleitungen an eine Verwaltungsstelle hatte in der Vergangenheit bereits vereinzelt zu Anfragen von Kursleitenden bei der Datenschutzstelle geführt; im Berichtsjahr war es jedoch die IF selbst, welche sich anlässlich einer internen Neuorganisation mit verschiedenen Fragen an die Datenschutzstelle wandte.
Die IF stellte der Datenschutzstelle in diesem Zusammenhang auch die von ihr verwendeten Unterlagen zur Durchsicht zu, welche sich an die externen Sprachkursanbieter bzw. deren Kursleitende richten. Die Kursleitenden haben mit einem Lernfeedbackformular (pro Kursteilnehmer) und einem (zusammenfassenden) Reportingblatt (pro Kursgruppe und Semester) Angaben zur Person der Teilnehmenden (Name, Vorname, Geburtsjahr, Muttersprache) und detaillierte Angaben zu deren sprachlichen Kenntnissen und Fähigkeiten bei Kursstart und Kursende (namentlich Vorkenntnisse und Lernfortschritt betreffend Hören, Lesen, Schreiben, sprachliche Interaktion und Produktion) zu erfassen und der IF nach Kursende zuzustellen.

Die Datenschutzstelle stellte fest, dass aus den Unterlagen nicht hervorging, zu welchem Zweck die IF von den externen Sprachkursanbietern bzw. deren Kursleitenden die Erhebung dieser Angaben zu den einzelnen Kursteilnehmenden verlangt und braucht. Dabei konnte die IF der Datenschutzstelle gegenüber auf Nachfrage hin darlegen, dass sie die erhobenen Daten der Kursteilnehmenden zum Zwecke der Kontrolle und Koordination braucht, welche sie im Rahmen der Gewährung eines Sprachförderkredits wahrzunehmen hat (also quasi im Gegenzug zu den Subventionen) und dass ihr ohne diese Angaben weder eine Steuerung noch eine Qualitätssicherung der Kursangebote möglich wäre. Da zudem durch die

[45] Bspw. Geburts- und Sterbedatum. [46] Die Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung besteht seit Inkrafttreten von Art. 321bis StGB im Jahre 1993. Sie erlässt Bewilligungen für einzelne Forschungsprojekte, für Spitäler und Institute sowie für Medizinalregister im Bereich der medizinischen Forschung; vgl. aber FN 48.
[47] www.bag.admin.ch, Expertenkommission Berufsgeheimnis/Bewilligungsarten.

[48] Gestützt auf das am 30 September 2011 von der Bundesversammlung verabschiedeten Humanforschungsgesetz (HFG) sollen allerdings die kantonalen Ethikkommissionen in Zukunft unter bestimmten Voraussetzungen Ausnahmebewilligungen im Bereich des Berufsgeheimnisses erteilen können. Die Eidg. Expertenkommission wird abgeschafft und Art. 321bis Abs. 2 StGB entsprechend angepasst.

IF keine Teilnehmerdaten weiter gegeben werden bzw. nur in Form von anonymisierten bzw. statistischen Daten an Bund und Kanton, beurteilte die Datenschutzstelle die von der IF verlangten Datenerhebungen durch die Sprachkursanbieter als nachvollziehbar und verhältnismässig. Die Datenschutzstelle empfahl jedoch, die an die externen Sprachkursanbieter bzw. deren Kursleitenden gerichteten Unterlagen betreffend Zweck und Weiterleitung zu ergänzen bzw. zu präzisieren.[49] Diese Anregung wurde von der IF umgehend umgesetzt.

15 Auskunft über Halbgeschwister durch Einwohnerkontrolle

Ein 80-jähriger Adoptivsohn, welcher seinen verstorbenen leiblichen Vater namentlich kannte, wollte vom Personenmeldeamt Auskunft aus dem Einwohnerregister über die Personalien von allfälligen Halbgeschwistern. Da sein leiblicher Vater zu Lebzeiten in Zürich angemeldet war, verfügt das Personenmeldeamt in seinen Archivbeständen über die ersuchten Informationen betreffend weiterer Kinder des Vaters. Das Personenmeldeamt wandte sich im Zusammenhang mit diesem Auskunftsgesuch an die Datenschutzstelle, da der Anspruch eines Adoptivkindes auf Auskunft über die Personalien allfälliger Halbgeschwister gesetzlich nicht klar geregelt ist.[50]

Das Gemeindegesetz verlangt für eine derartige Auskunft aus dem Einwohnerregister entweder eine ermächtigende Rechtsgrundlage oder die Einwilligung der Halbgeschwister.[51] Ein Anspruch des Adoptivsohns auf Kenntnis der Personalien allfälliger Halbgeschwister kann nach Ansicht der Datenschutzstelle aus dem in der Bundesverfassung festgeschriebenen Grundrecht der persönlichen Freiheit[52] sowie dem im Zivilgesetzbuch verankerten Persönlichkeitsrecht[53] hergeleitet werden. Das Personenmeldeamt ist daher grundsätzlich ermächtigt, dem Gesuchsteller die Personalien seiner Halbgeschwister bekannt zu geben, hat aber – soweit möglich und zumutbar – auch die Interessen der betroffenen Halbgeschwister zu berücksichtigen. Die Datenschutzstelle hat dem Personenmeldeamt deshalb empfohlen, vor einer Auskunftserteilung wenn immer möglich die betroffenen Halbgeschwister anzufragen, ob sie eine Kontaktaufnahme durch den Gesuchsteller wünschen oder nicht. Auch diese Information soll dann – analog zur Auskunftserteilung im Adoptionsrecht[54] – durch das Personenmeldeamt an die Gesuchstellenden (vorliegend den Halbbruder) weitergeleitet werden. Das Personenmeldeamt ist im vorliegenden Fall so vorgegangen und konnte dem Gesuchsteller die ersuchten Auskünfte über seine Halbgeschwister erteilen.

[49] Die Transparenz den Kursteilnehmenden gegenüber wird auf dem entsprechenden Formular geschaffen, indem über die Weiterleitung an den IF orientiert wird. [50] Im Gegensatz zum gesetzlich geregelten, bedingungslosen Anspruch eines volljährigen Adoptivkindes auf Auskunft über die Personalien seiner leiblichen Eltern (Art. 268c ZGB). [51] § 38 lit. a GG, LS 131.1. [52] Art. 10 BV. [53] Art. 28 ZGB. [54] Art. 268c Abs. 2 ZGB.

16 Telefonaufzeichnung am Arbeitsplatz

Der Schutz der Geheimhaltung und Vertraulichkeit von Telefongesprächen geniesst in der Schweiz hohen Stellenwert. Das Aufnehmen von Telefongesprächen ist denn auch grundsätzlich nicht erlaubt und strafbar.[55] Kein strafbares Verhalten liegt ausnahmsweise vor, wenn alle Beteiligten einwilligen oder wenn im Geschäftsverkehr die Aufnahme von Telefongesprächen zur Beweissicherung von Bestellungen, Aufträgen, Reservationen und ähnlichen Geschäftsvorfällen erfolgt.[56]

Mitarbeitende einer Dienstabteilung, in welcher Geschäftsabschlüsse branchenüblich in grosser Anzahl über Telefon getätigt werden, gelangten an die Datenschutzstelle mit der Bitte um Klärung und Beurteilung der Handhabung der Telefonaufzeichnungen an ihrem Arbeitsplatz. Die Zulässigkeit und Notwendigkeit von Telefonaufzeichnungen an ihrem Arbeitsplatz an sich haben die Mitarbeitenden nicht in Frage gestellt; vorgebracht wurde aber, dass keine Klarheit herrsche, welche Telefongespräche aufgezeichnet und in welchen Fällen zu welchen Zwecken die Aufzeichnungen ausgewertet würden. Entsprechende Anfragen seien von den Vorgesetzten unbeantwortet geblieben.

Auf Anfrage der Datenschutzstelle stellte sich heraus, dass in der betreffenden Dienstabteilung bereits seit einiger Zeit eine entsprechende Unternehmensweisung in Erarbeitung war. In der Folge führte die Datenschutzstelle mit Mitarbeitenden, dem Rechtsdienst und der Geschäftsleitung der betroffenen Dienstabteilung mehrere Beratungs- und Vermittlungsgespräche. Nach Ansicht der Datenschutzstelle enthält die zwischenzeitlich in Kraft getretene Unternehmensweisung die erforderlichen Regelungen; insbesondere legt sie fest,

- zu welchen Zwecken Telefonaufzeichnungen erfolgen und ausgewertet werden dürfen. Durch die abschliessende Erwähnung (insbesondere Beweissicherung telefonisch abgeschlossener Rechtsgeschäfte) ist gleichzeitig auch bestimmt, dass Telefonaufzeichnungen nicht zu Kontrollen von Verhalten am Arbeitsplatz verwendet werden dürfen;
- dass ein Zugriff auf Aufzeichnungen nur durch die zuständige Abteilungsleitung in Zusammenarbeit mit dem Rechtsdienst erfolgen darf und dass das Verfahren hierfür definiert ist;
- dass die Mitarbeitenden in transparenter Weise zu informieren sind: sowohl vorgängig über alle wesentlichen Modalitäten der Telefonaufzeichnungen durch Abgabe der Unternehmensweisung wie auch nachträglich über erfolgte Zugriffe auf Aufzeichnungen (sofern die betroffenen Mitarbeitenden nicht bereits vor dem Zugriff beigezogen werden konnten);
- dass allen Mitarbeitenden das Führen von Telefongesprächen, die nicht auf gezeichnet werden sollen, zu ermöglichen ist.

[55] Art. 179bis ff. StGB. [56] Art. 179quinquies StGB.

Diesem Sachverhalt liegt eine Problematik zu Grunde, welche regelmässig zu Anfragen bei der Datenschutzstelle führt[57]: die zunehmend omnipräsente Technologisierung des Arbeitsplatzes. Diese hat zur Folge, dass vermehrt elektronische Daten, die auch die Mitarbeitenden unmittelbar betreffen (können), anfallen bzw. erhoben werden und dadurch auch das Potential für Überwachungsmöglichkeiten steigt. Ist den Mitarbeitenden die Aufzeichnung und Verwendung von Daten nicht oder nicht genau bekannt und sind Aufzeichnungen damit weder nachvollzieh- noch kontrollierbar, kann dies zu Unbehagen am Arbeitsplatz oder gar Misstrauen den direkten Vorgesetzten gegenüber führen. Nicht anders verhielt es sich im vorliegenden Fall. Der Grund, weshalb sich die Mitarbeitenden an die Datenschutzstelle gewandt haben, war in erster Linie das Fehlen von Transparenz, Verbindlichkeit und somit schliesslich von Rechtssicherheit im Umgang mit den Telefonaufzeichnungen.

[57] Vgl. bspw. TB 2010, S. 20 ff. (Elektronische Badgesysteme); TB 2008, S. 20 f. (Tonbandaufzeichnungen bei Mitarbeitergesprächen).

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

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

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

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

Monika Niederberger
Sekretariat (20 %)

Stadt Zürich
Datenschutzbeauftragter
Beckenhofstrasse 59
8006 Zürich

Tel. 044 363 24 42
Fax 044 363 24 43

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