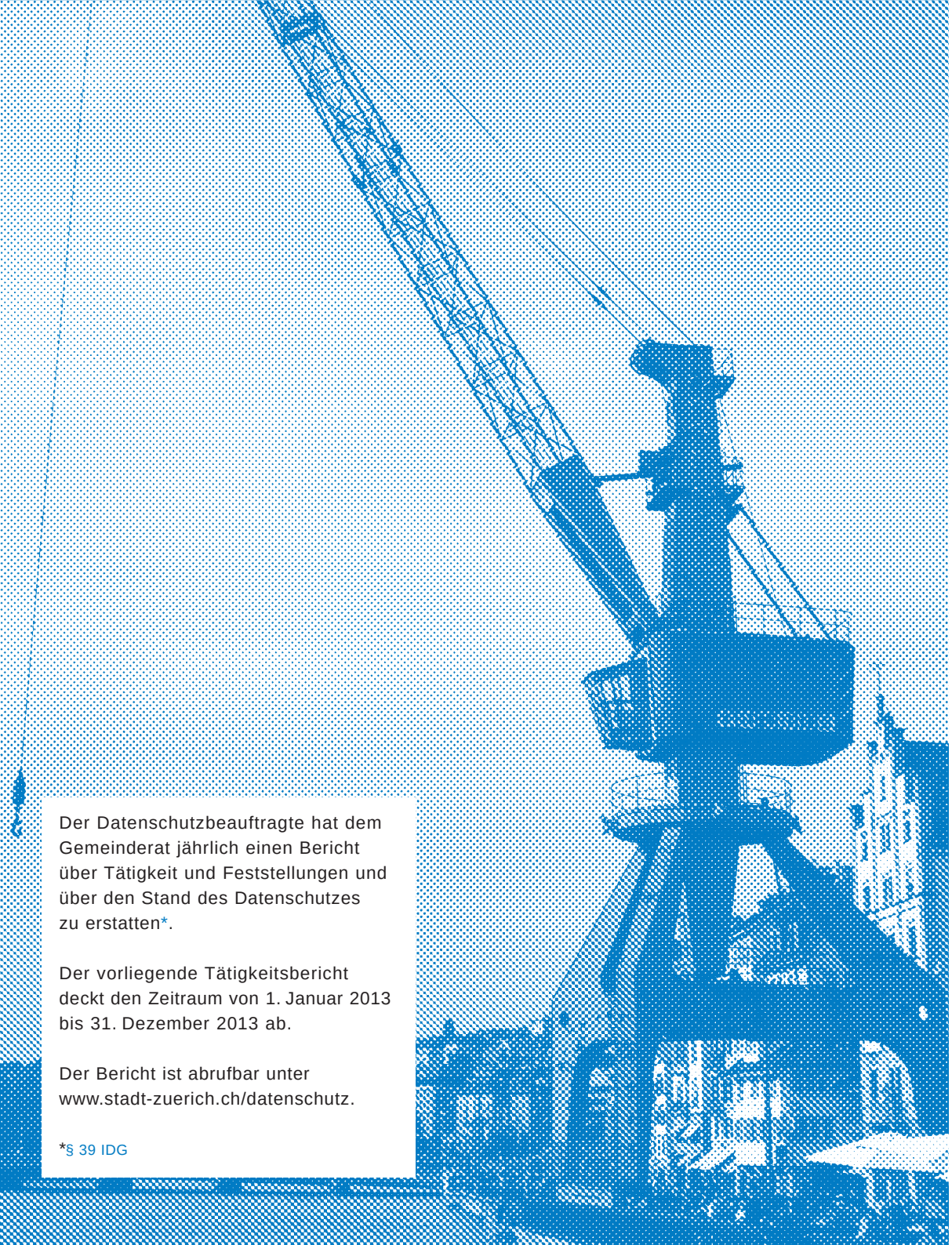
Stadt Zürich
Datenschutzbeauftragter

Tätigkeitsbericht 2013



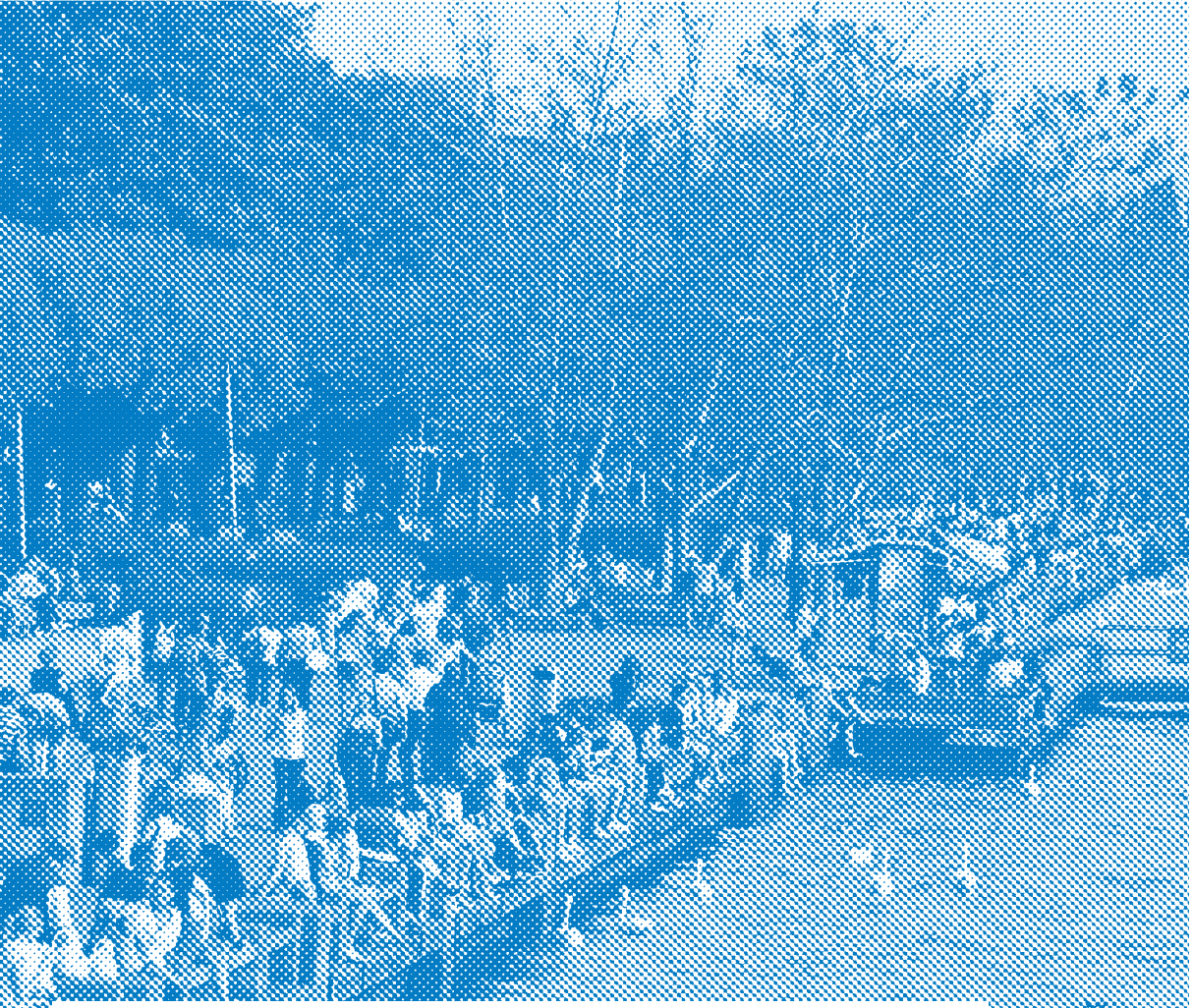
Der Datenschutzbeauftragte hat dem Gemeinderat jährlich einen Bericht über Tätigkeit und Feststellungen und über den Stand des Datenschutzes zu erstatten*.

Der vorliegende Tätigkeitsbericht deckt den Zeitraum von 1. Januar 2013 bis 31. Dezember 2013 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 2013

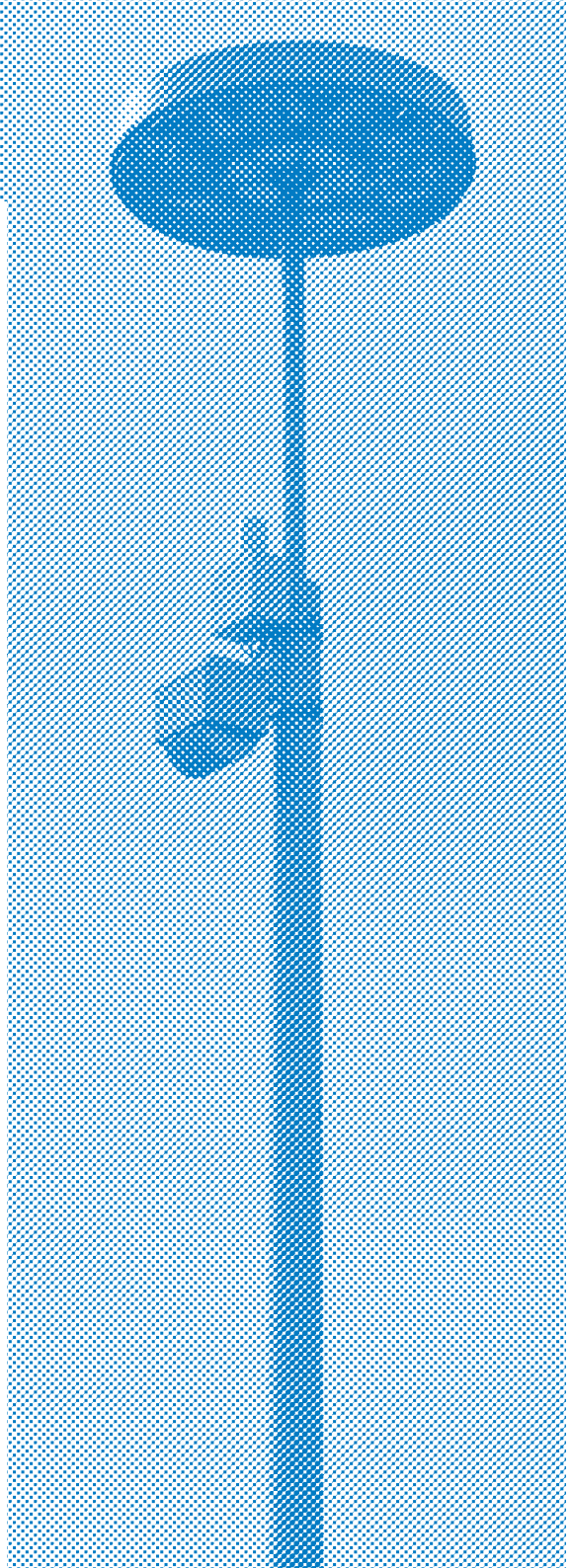
Nebst der Videoüberwachung, die im vorliegenden Tätigkeitsbericht das Schwerpunktthema darstellt, stand im Berichtsjahr der fach- und organisationsübergreifende Informationsaustausch als gesamtstädtisches Datenschutzthema im Vordergrund.

Die Tätigkeiten und Dienstleistungen von Verwaltungsstellen stehen oft in Beziehung oder Abhängigkeit mit denjenigen anderer öffentlichen oder privaten Stellen. Verlangt wird deshalb von der Verwaltung zunehmend eine vernetzte und interdisziplinäre Arbeitsweise, oftmals auch über Organisationsgrenzen hinweg. Eine solche Zusammenarbeit bringt mit sich, dass Informationen und Personendaten ausgetauscht werden müssen. Handelt es sich dabei um sensible Personendaten oder um Verwaltungsbereiche, die einer besonderen Geheimhaltung wie beispielsweise einem Berufsgeheimnis unterstehen, wird der Informationsaustausch nicht selten als eine äusserst komplizierte Angelegenheit betrachtet, die zu viel Unsicherheit und Verwirrung führt. In der Tat bringen derartige Konstellationen regelmässig komplexe rechtliche Fragestellungen mit sich, die unter Umständen nur mit viel Aufwand, auf alle Fälle aber nur mit entsprechendem Knowhow in Bezug auf die Aufgabenerfüllung der jeweiligen Verwaltungsstellen beantwortet werden können. Der Informationsaustausch, den eine fach- und organisationsübergreifende Kooperation mit sich bringt, ist keine von der übrigen Tätigkeit der involvierten Stellen losgelöste Thematik. Im Gegenteil, Zulässigkeit und Ausmass eines Informationsaustauschs ergibt sich in erster Linie aus der Bereichsgesetzgebung der jeweiligen Verwaltungsstellen und nicht aus allgemeinen Datenschutzbestimmungen. Der Informationsaustausch von Behörden kann deshalb auch nicht pauschal als Ganzes beurteilt werden, sondern muss in die einzelnen Kommunikationsteile zerlegt werden. Für jede beteiligte Stelle muss gesondert geprüft werden, welche Informationen mit wem aufgrund welcher Grundlagen ausgetauscht werden dürfen. Massgebend können dabei eine Vielzahl von Rechtsgrundlagen – sowohl der bekanntgebenden als auch der empfangenden Stellen – sein, die sich aus Bundes-, Kantons- oder Gemeinderecht ergeben können.

Die zahlreichen bereichsspezifischen Rechtsgrundlagen zu kennen, die den Informationsaustausch in der Verwaltung regeln, stellt je länger je mehr eine echte Herausforderung dar. So gesehen ist es verständlich, dass eine Antwort auf die Frage nach der Zulässigkeit bestimmter informationeller Kooperationen unter Umständen schwierig sein kann. Alternativen zu einzelfall- und kontextbezogenen Abklärungen gibt es aber nicht. Den verwaltungs-internen Informationsaustauch pauschal unter dem Titel «Amtshilfe» als zulässig zu erklären ist ebenso falsch wie ihn mit der Begründung «Datenschutz» bzw. «fehlende Rechtsgrundlage» weitgehend verhindern zu wollen. Auch der Bundesrat kommt in einem Bericht zum Austausch personenbezogener Daten zwi-

schen Behörden des Bundes und der Kantone zum Schluss, dass die Schwierigkeiten beim Datenaustausch oft nicht auf fehlende rechtliche Grundlagen zurückzuführen seien, sondern darauf beruhen, dass das Zusammenspiel der verschiedenen Normen geklärt und anschliessend den Rechtsanwendenden kommuniziert werden müsse.

Um die erforderlichen Prüfungen zu erleichtern, hat die Datenschutzstelle für einige Verwaltungsbereiche Übersichten erstellt, die im Sinne einer ersten Orientierungshilfe einen Überblick über vorhandene Rechtsquellen geben, die einen Informationsaustausch zum Gegenstand haben (können). Sie sollen dazu beitragen, die wichtigsten Grundlagen rasch auffindbar zu machen. Die Übersichten sind auf der Webseite der Datenschutzstelle publiziert, mit dem Hinweis, dass diese aber in keinem Falle eine einlässliche Prüfung relevanter Rechtsgrundlagen ersetzen können. Vom Thema Informationsaustausch geprägt bzw. auf dieses Thema fokussiert waren auch die Weiterbildungsveranstaltungen, die die Datenschutzstelle in jüngster Zeit in Zusammenarbeit mit diversen Verwaltungsstellen – aus den Bereichen Polizei, Schule, Soziales – durchgeführt hat.



II Themen

1 Videoüberwachung durch die Stadtverwaltung

Die Stadtverwaltung hat ungefähr 2'000 Videokameras im Einsatz. Was auf den ersten Blick nach Überwachungsstaat aussieht, relativiert sich bei genauem und differenziertem Hinschauen. Damit auch in Zukunft auf Stadtgebiet keine übertriebene Videoüberwachung stattfindet, müssen die Vernetzung der Systeme und die Überwachung öffentlichen Grundes durch Private im Auge behalten werden.

a) Vorgeschichte

Beginnen wir mit einem Blick zurück: Seit Oktober 2011 besteht für die Stadtverwaltung Klarheit, unter welchen Voraussetzungen sie Videoüberwachung einsetzen darf. Auf diesen Zeitpunkt hin trat die städtische Datenschutzverordnung (DSV) in Kraft, welche bestimmt, dass Videoüberwachung an neuralgischen Punkten mit erheblicher Gefahr für Leib, Leben oder Sachen eingesetzt werden darf. Sind diese Voraussetzungen erfüllt, so muss die zuständige Dienstabteilung für ihre Videoüberwachung in aller Regel ein Reglement erstellen und dieses der Datenschutzstelle zur Prüfung vorlegen. Die DSV gibt den wichtigsten Inhalt der Reglemente vor, ebenso wie die zeitliche Vorgabe, dass die Reglemente bereits bestehender Videoüberwachungen bis Oktober 2012 (hätten) vorliegen müssen.

Es hat sich gezeigt, dass die Stadtverwaltung für die Erarbeitung der Videoreglemente mehr Zeit als erwartet benötigt hat. Die Datenschutzstelle hat bereits in ihrem letztjährigen Tätigkeitsbericht darüber informiert, dass die vorgesehene Frist von zahlreichen Dienstabteilungen nicht eingehalten werden konnte. Nicht selten hat die Stadtverwaltung bei der Erarbeitung der Videoreglemente Komplexität und Aufwand – vor allem bezüglich Bereitstellung von Knowhow und Ressourcen im rechtlichen Bereich – unterschätzt. Zwischenzeitlich hat die Stadtverwaltung bis auf wenige Ausnahmen ihre Videoüberwachungen auf die Vereinbarkeit mit der revidierten städtischen DSV geprüft und die erforderlichen Videoreglemente erstellt.

b) Videoüberwachungen nach städtischer Datenschutzverordnung (DSV)

Die Stadtverwaltung Zürich hat 13 Reglemente für Videoüberwachungen erstellt und nach vorgängiger Prüfung durch die Datenschutzstelle in Kraft gesetzt. Gegen die amtlich publizierten Reglemente der Stadtverwaltung wurden keine Einsprachen erhoben.

Gestützt auf die städtische DSV haben derzeit 12 Dienstabteilungen rund 800 Kameras im Einsatz, die wie folgt kategorisiert bzw. unterschieden werden können:

- Mehr als die Hälfte dieser Kameras, rund 400 Stück, betreffen Örtlichkeiten, die erlaubterweise für die Öffentlichkeit

nicht zugänglich sind, so insbesondere kritische Infrastrukturen, Werke und Anlagen in den Bereichen Elektrizität, Wasserversorgung oder Entsorgung.

- Zur Überwachung des Stadions Letzigrund werden rund 60 Kameras eingesetzt. Bei Grossveranstaltungen hat das Stadion erhöhten Sicherheitsanforderungen zu genügen. Videoüberwachung stellt dabei eine zentrale Massnahme dar.
- Die beiden Stadtspitäler haben circa 80 Kameras im Einsatz. Der grösste Teil dieser Kameras zeichnet keine Bilder auf, sondern dient lediglich einem live-Monitoring (bspw. in Korridoren zwecks Patientensicherheit) oder einer Bildübertragung auf Abruf (bspw. als Türsprechfunktion). Aufzeichnungen erfolgen für die Überwachung der Tiefgarage.
- Die Stadtpolizei setzt für die Überwachung ihrer Immobilien und Verwaltungsgebäude circa 125 Kameras ein. Bildaufzeichnungen erfolgen bei weniger als der Hälfte dieser Kameras und nur anlassbezogen, d.h. nicht permanent, sondern nur bei Ereignissen mit entsprechendem Gefährdungspotential für Polizeigebäude.
- Für die Videoüberwachung in den übrigen Verwaltungsgebäuden der Stadtverwaltung ist mit wenigen Ausnahmen die Dienstabteilung Immobilienverwaltung (IMMO) zuständig, da ihr auch die übrige Bewirtschaftung dieser Liegenschaften obliegt. Die IMMO setzt hierfür circa 135 Kameras ein. Die Verwaltungsgebäude werden ausschliesslich ausserhalb der Öffnungszeiten, nur an definierten Orten (Eingangsbereiche, Etagenzugänge) und nur im Falle von unberechtigten Zutrittsversuchen überwacht. Eine Überwachung des Publikums in den Verwaltungsgebäuden der Stadtverwaltung findet nicht statt. Einzige Ausnahme ist ein Schalterbereich, der aus Sicherheitsgründen auch während den Öffnungszeiten überwacht werden muss.

Sonderfall Schulgebäude und Schulanlagen

Bereits im Jahre 2009 hat der Stadtrat ein Reglement für den Einsatz von Videoüberwachung bei Schulgebäuden und -anlagen erlassen (AS 410.200). Zu diesem Zeit punkt war zwar bekannt, dass die städtische Datenschutzverordnung (DSV) revidiert und dem neuen kantonalen Informations- und Datenschutzgesetz (IDG) angepasst werden muss. Nicht bekannt war jedoch, ob und mit welcher materiellen Regelung der Gemeinderat Bestimmungen zur Videoüberwachung in die städtische DSV aufnehmen wird. Die Sonderregelung für den Bereich der Schulgebäude durch den Stadtrat musste deshalb so zurückhaltend und restriktiv ausfallen, dass sie nicht in Widerspruch mit einer allfälligen nachfolgenden Regelung durch den Gemeinderat stehen würde. Um diese Kompatibilität sicherzustellen, wurde nebst einer einschränkenden Zweckbestimmung grossen Wert auf eine konkrete und abschliessende Definition von Umfang und Art der Videoüberwachung bei Schulgebäuden gelegt. Gestützt auf das stadträtliche Reglement darf Vdeoüberwachung nur zum Schutz von Gebäuden und An-

lagen eingesetzt werden und steht somit nicht für beliebige weitere, beispielsweise schulische Zwecke zur Verfügung. Das Reglement hält weiter fest, dass nur Gebäude-Aussenfassaden sowie abschliessbare Sport- und Freizeitanlagen überwacht werden dürfen und dass eine Überwachung nur zu Zeiten, während denen die Schulgebäude und -anlagen nicht zur Benutzung zur Verfügung stehen, zulässig ist.

Bei Schulgebäuden und Schulanlagen der Stadt Zürich stehen rund 600 Kameras in circa 20 Schulanlagen im Einsatz. Für das Jahr 2014 ist ein Ausbau im Umfang von weiteren circa 200 Kameras vorgesehen.

c) Weitere Videoüberwachungen durch die Stadtverwaltung

Die Stadtverwaltung muss nicht für jede Videoüberwachung ein Reglement gemäss städtischer DSV erstellen. Überall dort, wo die Stadtverwaltung gestützt auf bereichsspezifische Rechtsgrundlagen – sei es auf Bundes-, kantonaler oder kommunaler Ebene – Videoüberwachung einsetzen darf, richten sich die materiellen Voraussetzungen und allfällige formelle Vorschriften nach diesen Grundlagen. Die wichtigsten Videoüberwachungen durch die Stadtverwaltung ausserhalb des Geltungsbereichs der städtischen DSV sind folgende:

Videoüberwachung im öffentlichen Verkehr

Seit dem Jahre 2010 gilt für die Videoüberwachung in den Trams und Bussen der VBZ ausschliesslich Bundesrecht. Die Bundesverordnung über die Videoüberwachung im öffentlichen Verkehr bestimmt, zu welchen Zwecken Videoüberwachung eingesetzt werden darf und nach welchen Modalitäten mit Aufzeichnungen umzugehen ist. Seither stehen der städtischen Datenschutzstelle gegenüber der VBZ im Bereich des öffentlichen Verkehrs auch keine Aufsichts- oder Beratungsaufgaben mehr zu. Zuständig hierfür ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

Gemäss Auskunft der VBZ stehen für die Überwachung stationärer Anlagen auf Stadtgebiet rund 130 Kameras im Einsatz. Hinzuzurechnen sind die Kameras in den Trams und Bussen.

Videoüberwachung des Strassenverkehrs

Zum Zwecke der Überwachung bzw. des Managements des Strassengeschehens werden Kameras eingesetzt. Diese liefern Übersichtsbilder, die datenschutzrechtlich nicht relevant sind, da auf ihnen weder Personen noch Nummernschilder erkannt werden können. Aufzeichnungen erfolgen keine.

Die städtische Dienstabteilung Verkehr hat stadtweit Zugriff auf 85 Kameras, für welche grösstenteils die Kantonspolizei Zürich zuständig ist.

Videoüberwachung bei Grossanlässen

Die Stadtpolizei Zürich weist auf ihrer Webseite darauf hin, dass an den vier Standorten Stadthausquai, Bürkliplatz, Bellevue und Bernhardtheater Kameras zwecks Gewährleistung der öffentlichen Sicherheit fest installiert sind. Dabei wird darauf hingewiesen, dass die Videoüberwachung nur anlässlich von Grossveranstaltungen und Kundgebungen eingesetzt wird und während der übrigen Zeit ausser Betrieb ist. Rechtsgrundlage für diese Videoüberwachung bilden revidierte Bestimmungen des kantonalen Polizeigesetzes, die im März 2013 in Kraft getreten sind. Regelungen betreffend Einsatz, Zuständigkeit und Umgang mit Videobildern hat die Stadtpolizei in einer internen Dienstanweisung erlassen.

Multikopter

Die Stadtpolizei hat im Berichtsjahr zusammen mit der Dienstabteilung Geomatik+ Vermessung (GeoZ) einen sogenannten Multikopter angeschafft. Auch wenn solche Fluggeräte nicht für Videoüberwachung eingesetzt werden, gelten sie dennoch geradezu als Sinnbild für Überwachung und Kontrolle. Bei der Stadtpolizei ist der Einsatz des Multikopters in erster Linie auf Aufgaben des unfalltechnischen Dienstes, d.h. auf das Erstellen von Fotografien von Unfallorten, beschränkt. Ausdrücklich ausgeschlossen sind Einsätze im Rahmen von Demonstrationen, Festen und Veranstaltungen. GeoZ setzt den Multikopter für die Erstellung von Orthofotos sowie digitaler Oberflächen und Geländemodelle ein. Für alle diese Einsatzzwecke gilt, dass ein Aufzeichnen von Personen auf den Bildern unerwünscht und störend wäre, so dass darauf geachtet wird, möglichst von Beginn an keine Personen zu erfassen. Sollte dies dennoch geschehen, werden die entsprechenden Rohbilder anonymisiert. Der Gebrauch von Multikoptern für derartige Einsätze ist deshalb von geringer datenschutzrechtlicher Relevanz. Sowohl die Stadtpolizei als auch GeoZ haben den Anwendungsbereich des Multikopters mit interner Dienstanweisung bzw. internem Reglement verbindlich geregelt.

d) Beurteilung der Datenschutzstelle

Aus Sicht der städtischen Datenschutzstelle kann gut drei Jahre nach Einführung der Videobestimmungen in der städtischen DSV ein positives Fazit gezogen werden, auch wenn der damit verbundene Aufwand – sowohl für die verantwortlichen Dienstabteilungen als auch für die Datenschutzstelle – unterschätzt wurde. Es hat sich schon bald gezeigt, dass der Bedarf an fachlicher Unterstützung bei der Erstellung der Reglemente und insbesondere auch bei den hierfür erforderlichen juristischen und faktischen Vorarbeiten zu gross war, als dass sich die Datenschutzstelle auf eine blosse Prüfung der Reglemente hätte beschränken können.

Mit der Einführung der Reglementspflicht gemäss DSV setzte der städtische Gesetzgeber nicht nur rechtliche Hürden, sondern verlangte in erster Linie die Schaffung von Transparenz. Wer von einer Videoüberwachung durch die Stadtverwaltung betroffen ist, soll anhand der verlangten Reglemente erkennen können, wo, wann, in welcher Weise und in welchem Ausmass in seine grundrechtlich geschützte Privatsphäre eingegriffen wird. Mit den publizierten und auf den Webseiten der jeweiligen Verwaltungsstellen zugänglichen Reglementen wird dieses Ziel erreicht. Die Videobestimmungen des städtischen Gesetzgebers haben aber nicht nur zu mehr Transparenz, sondern vor allem auch zu

einem veränderten Bewusstsein für und einem andern Umgang mit Videoüberwachung geführt. Die bestehenden Videoüberwachungen wurden seitens Stadtverwaltung früher oft in erster Linie als ein Thema des technischen «Handlings» wahrgenommen und behandelt. Mit der Revision der DSV rückten rechtliche Aspekte in den Vordergrund, die mit sich brachten, dass sich auch die Rechtsdienste oder die Führungsebenen der jeweiligen Verwaltungsstellen mit dem Thema Videoüberwachung auseinandersetzen mussten: Wer weiterhin oder neu Videoüberwachung einsetzen will, muss für seinen Verwaltungsbereich die rechtlichen Voraussetzungen (erhebliche Gefahr für Leib, Leben oder Sachen, neuralgische Punkte) prüfen und beurteilen, die vorgesehene Videoüberwachung einer kritischen Verhältnismässigkeitsprüfung unterziehen und schliesslich ein verbindliches Reglement erlassen, welches durch die Datenschutzstelle auf Einhaltung der Voraussetzungen geprüft wird. Zu guter Letzt hat die Erarbeitung der Reglemente für die bereits bestehenden Videoüberwachungen auch dazu geführt, dass zahlreiche Dienstabteilungen ihren bisherigen Einsatz reduziert haben, beispielsweise indem sie auf bestimmte Überwachungen oder Kamerastandorte ganz oder bei gewissen Kameras mindestens auf eine Aufzeichnung von Bildern verzichtet haben.

Mehr als die Summe aller Einzelteile

Auch wenn die Gesamtzahl der in der Stadtverwaltung eingesetzten Kameras auf den ersten Blick hoch erscheinen mag, ein genauer und differenzierter Blick zeigt, dass – zumindest heute noch – nur wenige Einsätze von Videoüberwachung aus Sicht Persönlichkeits- oder Datenschutz eine erhöhte Sensibilität aufweisen. Den Grundstein dafür legte der Gemeinderat in der städtischen Datenschutzverordnung mit der restriktiven Regelung betreffend Voraussetzungen von Videoüberwachung sowie der Reglementspflicht. Dass Videoüberwachung dennoch weiterhin auf der politischen Agenda bleiben muss, zeigen insbesondere Gegenstand und Grenzen der verlangten Prüfungen. Für die Beurteilung der Videoüberwachung wird jeder einzelne Einsatz gesondert betrachtet. Der Blick fällt also stets auf die jeweilige Anwendung bzw. den jeweiligen Einzelfall und nicht auf die Gesamtmenge. Aus (datenschutz-) rechtlicher Optik ist somit massgebend, dass jede einzelne Videoüberwachung sich auf eine gesetzliche Rechtfertigung abstützen kann und in Relation auf den verfolgten Zweck verhältnismässig, also als Massnahme geeignet und im Ausmass erforderlich, ist. Wie viele Videoüberwachungen zu anderen Zwecken und von anderen Stellen eingesetzt werden, ist dabei nicht von Relevanz. Dies mag gerechtfertigt sein, solange die einzelnen Einsätze von Videoüberwachung für sich stehen und voneinander unabhängig sind. Sollte aber diese Trennung aufgeweicht oder gar aufgehoben werden, besteht das Risiko, dass Videoüberwachung künftig tatsächlich zu dem wird, für was sie bereits seit längerem steht: nämlich für Überwachung im Stil von «big brother». Dieses Risiko besteht nicht nur aufgrund der Technik, welche laufend zu mehr Identifikation, Authentifikation und Vernetzung führt, sondern kann auch durch «fahrlässige» Gesetzgebung, die der Zweckbindung von Datenbearbeitungen und damit der informationellen Trennung zu wenig Wert beimisst, verstärkt werden. Je mehr im Bereich der Videoüberwachung diese Schranken durch den Gesetzgeber durchlässig gemacht werden, desto mehr besteht dieselbe Gefahr, die der Europäische Gerichtshof aktuell zur Vorratsdatenspeicherung im Telekommunikationsbereich gerügt hat: Videoüberwachung führt dann dazu, dass bei den Bürgerinnen und Bürgern das Gefühl erzeugt wird, ihr Privatleben sei Gegenstand einer ständigen Überwachung. Für den Blick auf's Ganze stehen deshalb auch Politik und Gesetzgeber in der Verantwortung, so wie dies beispielsweise mit einem aktuellen Postulat (GR-Nr. 2014/111) verlangt wird, welches die Überprüfung und Reduktion der Anzahl Videokameras an Schulgebäuden fordert.

Nebst der Vernetzungsproblematik ist noch eine weitere Facette der Überwachung von öffentlichem Grund im Auge zu behalten, nämlich diejenige Überwachung, die nicht durch die Stadtverwaltung, sondern durch Privatpersonen geschieht.

Videoüberwachung von öffentlichem Grund durch Private

Die Datenschutzstelle der Stadt Zürich erhält regelmässig Anfragen zum Thema Videoüberwachung von öffentlichem Raum durch Privatpersonen. Anlass für diese Anfragen sind die privaten Kameras, welche den öffentlichen Grund (mit)erfassen, beispielsweise bei Ladenlokalen, Restaurants und Geschäftsräumen, bei welchen nicht nur der Innenraum, sondern auch der Eingangsbereich und der umliegende öffentliche Raum gefilmt werden. Zweifellos tangiert die private Videoüberwachung die Privatsphäre der gefilmten Personen und engt in diesem Sinne den öffentlichen Raum zunehmend ein. Es besteht somit ein Konfliktpotential zwischen dem Interesse, den öffentlichen Raum zu nutzen, ohne dabei beobachtet und aufgezeichnet zu werden, und dem Interesse, für eigene Belange auch den öffentlichen Raum mittels Videoüberwachung mit einzubeziehen. Zum Schutz eigener Rechtsgüter bzw. aus Sicherheitsinteressen beziehen Private bestimmte Teilausschnitte des öffentlichen Raums in ihre Überwachungen mit ein. Eine solche Überwachung ist jedoch nur ausnahmsweise und in Einzelfällen zulässig, namentlich dann, wenn eine Überwachung zum Schutz hochrangiger Rechtsgüter, wie Eigentum oder Leib und Leben, geradezu unerlässlich ist und eine erhebliche Gefährdung besteht oder der Schutz besonders gefährdeter Einrichtungen bezweckt ist. Die Überwachung eines Ausschnitts aus dem öffentlichen Raum kann zum Schutz besonders gefährdeter Räumlichkeiten wie Banken oder Schmuckgeschäften zulässig sein. Sicherzustellen ist aber, dass die Überwachung nur eng begrenzte Ausschnitte des öffentlichen Raums erfasst, also insbesondere nur den unmittelbar an die Hausfassade angrenzenden Bereich des Trottoirs. Es dürfen nur diejenigen Personen erfasst werden, die unmittelbar an das Schaufenster oder die Fassade treten. Wird öffentlicher Raum nur in geringfügiger Weise tangiert und ist

dies für die Überwachung des privaten Grundes bzw. für den Schutz privater Interessen unerlässlich, wird dies in der Regel, auch aus Gründen der Praktikabilität, akzeptiert (vgl. dazu das entsprechende Merkblatt auf der Website des EDÖB).

Videoüberwachung durch Private wird durch das Privatrecht geregelt. Für Fragen des Datenschutzrechts kommt deshalb das Eidgenössische Datenschutzgesetz (DSG) zur Anwendung, mit der aufsichtsrechtlichen Zuständigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Im öffentlichen Recht ist die Problematik der Videoüberwachungen im öffentlich zugänglichen Raum durch Private bis heute weitgehend nicht geregelt. Auch das öffentliche Recht des Kantons Zürich bzw. der Stadt Zürich äussert sich hierzu nicht. Diese Situation scheint unbefriedigend, nicht zuletzt auch deshalb, weil sich Betroffene nur auf dem Zivilweg gegen Betreiber solcher Kameras wehren können.

Als möglicher Vorschlag, wie dem Problem der Videoüberwachung des öffentlichen Raums durch Private begegnet werden könnte, wird in der Rechtslehre die Einführung einer Bewilligungspflicht diskutiert. Dies mit der Begründung, dass es sich hierbei um gesteigerten Gemeingebrauch handle, da eine Inanspruchnahme öffentlichen Raums mittels Videoüberwachung durch Private nicht bestimmungsgemäss (öffentliche Strassen und Plätze sind zum Gehen, Fahren und für gewisse kommerzielle Tätigkeiten da) und auch nicht gemeinverträglich (andere Personen werden durch die Überwachung in der Nutzung des öffentlichen Raums tangiert) ist. Befürworter dieses Lösungsansatzes sind der Ansicht, dass damit die Position des Einzelnen bei der Verteidigung seiner Privatsphäre gestärkt werden könne. Die Lösung, für Installationen einer Videokamera eine Bewilligung für gesteigerten Gemeingebrauch zu verlangen, würde – so die Befürworter – richtigerweise das Augenmerk auf die zunehmende Einengung des öffentlichen Raumes durch private Überwachungsanstrengungen richten.

Eine nicht repräsentative Umfrage der städtischen Datenschutzstelle bei einigen kantonalen Berufskolleginnen und -kollegen hat gezeigt, dass in der Praxis die Möglichkeit der Bewilligung für gesteigerten Gemeingebrauch bei Videoüberwachung von öffentlichem Raum durch Private bis heute nicht angewendet wird. Einerseits, da deren Umsetzbarkeit in Zweifel gezogen wird und andererseits, weil die verwaltungsrechtliche Qualifikation der Überwachung von öffentlichem Grund durch Private umstritten ist. Auch nach Ansicht der städtischen Datenschutzstelle erscheint eine blosse Bewilligungspflicht als wenig überzeugend oder zielführend. Sollte Videoüberwachung durch Private vermehrt die Nutzung öffentlichen Grundes beeinträchtigen oder einschränken, wäre es wohl sinnvoller, umfassend zu prüfen, inwiefern sie zum Gegenstand öffentlichen Rechts erklärt, d.h. öffentlich rechtlich geregelt werden muss.

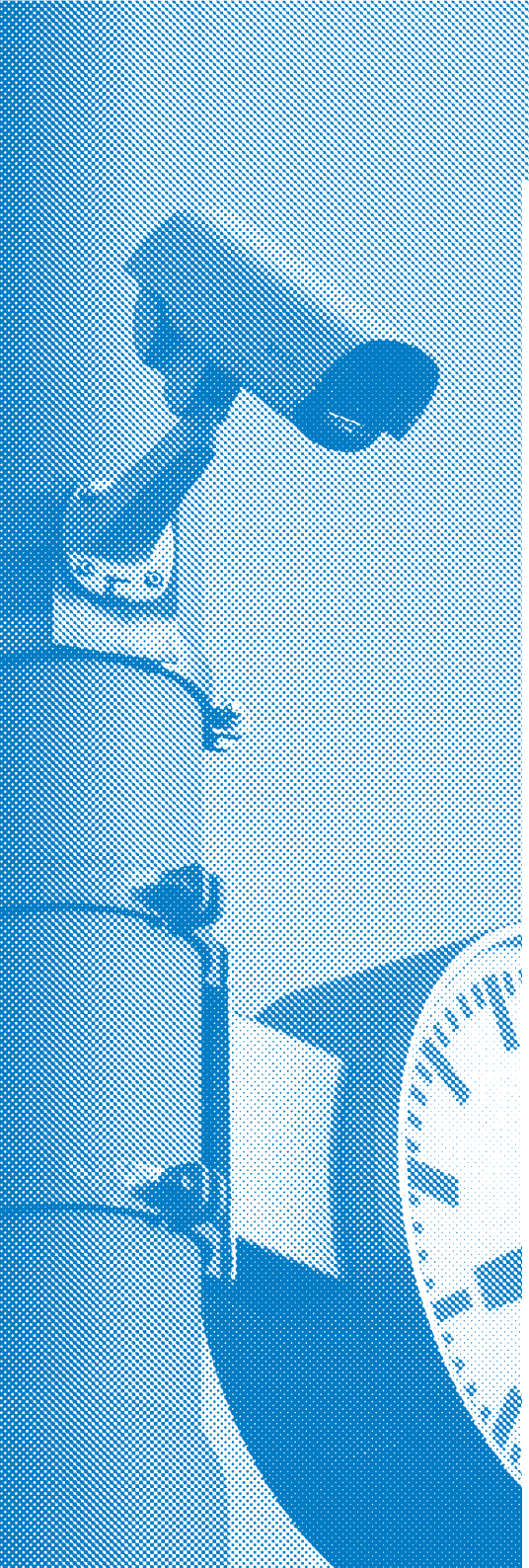
2 Bedrohungsmanagement

Vorbeugen ist besser als heilen. Was für unsere Gesundheit schon seit langem gilt, soll vermehrt auch für unsere Sicherheit gelten. Durch Früherkennung von Risiken sollen schwere Gewalttaten verhindert werden. Der Ruf nach Prävention stellt die polizeilichen Aufgaben und die sich daraus ergebenden Informationsbearbeitungen vor neue Herausforderungen.

Geschehen schwere Gewaltverbrechen, wird die Polizei heutzutage unweigerlich mit der Frage konfrontiert, ob diese nicht hätten verhindert werden können. Polizeiliche Tätigkeit hat nicht nur die Verfolgung und Ahndung begangener Straftaten, sondern vermehrt die Verhinderung zukünftiger Delikte zum Ziel. Im Fokus stehen dann nicht Strafen und Sanktionen, sondern Massnahmen zur Verhinderung potenzieller Sicherheitsgefährdungen.

Unter der Bezeichnung Bedrohungsmanagement setzen in- und ausländische Polizeien Analyseinstrumente zur Einschätzung von Risiken von Gewalttaten durch Einzelpersonen oder Gruppen ein. Mittels standardisierten Screeningverfahren sollen jene Fälle aus der Masse von Gewaltvorfällen herausgefiltert werden, bei denen schwere oder gar tödliche Gewalt drohen. Anschliessende vertiefte Analysen dienen dazu, die Risikoeinschätzungen zu präzisieren und spezifische Risikofaktoren zu identifizieren. Auf diese Bedrohungsanalysen folgt dann in der Regel ein Massnahmemanagement, welches mit anerkannten Strategien zur Deeskalation, zur Verhinderung von Straftaten oder zur Entschärfung von Risiken beitragen soll. Die von den Polizeikorps eingesetzten Instrumente werden von Universitäten oder spezialisierten Instituten entwickelt und vertrieben. Bereits werden fachliche Ausbildungen zur Funktion als Präventionsmanager mit entsprechender Zertifizierung angeboten.

Mit zunehmendem Anspruch nach frühzeitiger Erkennung von Eskalationspotential und Verhinderung möglicher Risiken wird sich die polizeiliche Tätigkeit von der Intervention und Repression vermehrt auch hin zur Prävention verschieben. Verändern wird sich nicht nur der Stellenwert, sondern auch das Ausmass präventiver Polizeitätigkeit. Das polizeiliche Interesse wird in grösserem Masse auf Individuen zielen, die als potentielle Täter erkennbar sind. Aufgaben und Kompetenzen der Polizei im Rahmen des Bedrohungsmanagements müssen sich in erster Linie aus der kantonalen (und allenfalls kommunalen) Polizeigesetzgebung ergeben. Das Polizeigesetz des Kantons Zürich zählt die Prävention zu den polizeilichen Aufgaben, jedoch bloss in allgemeiner und weitgehend unbestimmter Weise. Aus datenschutzrechtlicher Sicht drängt sich damit die Frage auf, ob das Polizeirecht den verlangten Anforderungen entspricht. Die Daten, die für präventive Polizeiaufgaben bearbeitet werden, haben als sensibel zu gelten und das Bedrohungsmanagement verlangt per definitionem eine interdisziplinäre und organisationsübergreifende Zusammenarbeit. Für die Bearbeitung derartiger Informatio-



nen werden genügend präzise Regelungen durch den Gesetzgeber verlangt. Und auch die Frage nach dem «wie viel» an Daten lässt sich schliesslich nur beantworten, wenn die gesetzlichen Aufgaben der Polizei im Bereich Bedrohungsmanagement mit einer gewissen Klarheit definiert sind.

Die rechtliche Problematik ist erkannt. Auf Bundesebene sind bereits mehrere Motionen und Postulate zu den Themen Gewaltprävention bzw. Bedrohungsmanagement eingereicht worden, unter anderem auch mit der Forderung nach einem Grundlagenbericht zum Bedrohungsmanagement bei häuslicher Gewalt mit speziellem Fokus auf den Datenaustausch. Der Bundesrat stellte im August 2013 in Aussicht, einen solchen Bericht in Zusammenarbeit mit den Kantonen zu erstellen.

Auch auf kantonaler Ebene sind entsprechende Abklärungen und Prüfungen im Gange. Der Datenschutzbeauftragte der Stadt Zürich hatte die Gelegenheit, die spezifisch datenschutzrechtlichen Grundlagen und Prüfkriterien in eine kantonale Arbeitsgruppe einzubringen. Dabei hat er darauf hingewiesen, dass eine Prüfung umfassend und mit Fokus auf jede involvierte Stelle erfolgen muss. Geprüft werden müssen alle bereichsspezifischen Rechtsgrundlagen sämtlicher Behörden, die im Rahmen eines Bedrohungsmanagements Informationen liefern oder erhalten sollen. Aus diesen Grundlagen haben sich die Antworten darauf zu ergeben, ob ein Recht oder gar eine Pflicht für einen Datenaustausch besteht, ob eine Datenbekanntgabe von sich aus oder nur auf Anfrage hin erfolgen darf und ob besondere Geheimhaltungs- oder Schweigepflichten bestehen, die erhöhte Anforderungen an einen Informationsaustausch mit anderen Stellen mit sich bringen oder einen solchen sogar gänzlich ausschliessen. Erst wenn die bereichsspezifischen Grundlagen der jeweiligen Verwaltungsstellen bekannt und geprüft sind, kann beurteilt werden, ob ein Informationsaustausch stattfinden darf und ob ein solcher allenfalls auch unter dem Titel der allgemeinen Amtshilfe zulässig wäre.

Die rechtliche Ausgangslage für die polizeilichen Tätigkeiten im Bereich Bedrohungsmanagement ist – insbesondere in Bezug auf den Informationsaustausch – offenbar noch wenig geklärt. Auch wenn die erforderlichen Prüfungen und Analysen primär auf Bundes- und kantonaler Ebene durchzuführen sind, steht die Stadtpolizei für ihr Bedrohungsmanagement, das sie selber definiert und betreibt, hinsichtlich Prüfung der rechtlichen und organisatorischen Anforderungen entsprechend in der Verantwortung. Die Datenschutzstelle hat die Stadtpolizei in den vergangenen Jahren wiederholt darauf hingewiesen und empfohlen, für das städtische Bedrohungsmanagement eine Analyse zu erstellen, die Auskunft über die faktischen und rechtlichen Grundlagen der wichtigsten Tätigkeiten und Informationsbearbeitungen gibt. Je sensibler Datenbearbeitungen sind, desto höher sind auch die Ansprüche an allfällige organisatorische Massnahmen. Sicherzustellen ist insbesondere, dass die wichtigsten Modalitäten der Datenbearbeitungen klar, nachvollziehbar und verbindlich geregelt sind. Gewährleistet werden muss auch, dass betroffene Personen das ihnen nach Datenschutzrecht zustehende Auskunftsrecht geltend machen können. Ob und welche organisatorischen Massnahmen für das Bedrohungsmanagement der Stadtpolizei erforderlich sein werden, kann erst nach Vorliegen einer genügend aussagekräftigen Analyse bzw. Beschreibung der Informationsbearbeitungen erfolgen.

3 Milieu-Datenbank der Stadtpolizei (MIDA)

Prostitution ist in der Stadt Zürich seit Januar 2013 bewilligungspflichtig. Die Datenschutzstelle hat die elektronische Datenbank mit dem Namen MIDA, die von der Stadtpolizei zur Administration der Bewilligungen geführt wird, auf die Einhaltung der datenschutzrechtlichen Anforderungen hin geprüft.

Der Stadtrat hat die Bestimmungen der Prostitutionsgewerbeverordnung der Stadt Zürich (PGVO) per Juli 2012 und Januar 2013 in Kraft gesetzt. Gestützt auf diese rechtliche Grundlage führt die Stadtpolizei eine sogenannte Milieu-Datenbank (MIDA). Im Berichtsjahr hat die Datenschutzstelle MIDA auf Umsetzung und Einhaltung der datenschutzrechtlichen Anforderungen hin überprüft.

Die PGVO beinhaltet zahlreiche Bestimmungen, welche für die Erfassung und die weitere Bearbeitung von Personendaten in MIDA massgebend sind. Ausgangspunkt ist die Zweckbestimmung, wonach die Daten, die gestützt auf die PGVO erhoben werden, für die Administration von Bewilligungen verwendet werden dürfen. Als weitere Verwendungszwecke werden die Identifikation von Opfern von Zwangsprostitution und der Nachweis von Urkundenfälschungen oder Falschlegitimationen genannt. Weiter bestimmt die PGVO, dass die Daten von den übrigen polizeilichen Daten getrennt bearbeitet werden müssen und dass sie spätestens fünf Jahre nach Erfassung zu löschen sind. Der Zugriff auf die Daten in MIDA ist auf Polizeiangehörige im Zuständigkeitsbereich Milieu- und Sexualdelikte zu beschränken. Welche Daten im Einzelnen von der Stadtpolizei in MIDA erfasst werden dürfen, wird nicht ausdrücklich in der PGVO erwähnt. Wie die Datenschutzstelle bereits im Entstehungsprozess der PGVO festgehalten hat, konnte auf eine derartige Definition auf formell-gesetzlicher Stufe verzichtet werden, da sich die erforderlichen Daten bzw. Datenkategorien bereits aus den übrigen Bestimmungen in genügendem Masse erkennen lassen.

Die Datensammlung MIDA steht der Stadtpolizei wie erwähnt in erster Linie zwecks Administration der (gemäss PGVO persönlichen) Bewilligungen zur Verfügung. In Bezug auf Informationen über betroffene Personen ergibt sich aus dieser Zweckbestimmung erst einmal eine Einschränkung der Datenerhebung auf Informationen zum Zwecke ausreichender Identifikation betroffener Personen. Des Weiteren müssen sogenannte Administrativdaten bearbeitet werden, wozu auch die Dokumentation erfolgter Kontrollen gehört. Auch lassen die einzelnen Bewilligungsvoraussetzungen, die in der PGVO ausdrücklich und abschliessend aufgezählt sind (bspw. Handlungsfähigkeit, Aufenthaltsrecht, Nachweis Krankenversicherung), in genügend klarer Weise erkennen, welche Daten hierfür von der Polizei erhoben werden dürfen bzw. müssen. Die PGVO räumt somit der Stadtpolizei in Bezug auf die erforderliche Datenerhebung und -bearbeitung einen begrenzten Handlungsspielraum ein, welchen sie mit pflichtgemässem Ermessen auszuüben hat. Für die Erhebung und Verwendung von Daten im System MIDA auch massgebend ist die Feststellung, dass mit der PGVO der Stadtpolizei keine zusätzlichen polizeilichen Kompetenzen für das Handeln im Bereich des Prostitutionsgewerbes geschaffen werden. Die hierfür relevanten Rechtsgrundlagen sind nach wie vor die schweizerische Strafprozessordnung sowie das kantonale und kommunale Polizeirecht.

Die Datenschutzstelle konnte feststellen, dass sich die in MIDA erfassten Daten auf die Zweckbestimmungen der PGVO abstützen lassen und insofern den gesetzlichen Anforderungen entsprechen. Nur beschränkt Auskunft konnte der Datenschutzstelle darüber erteilt werden, wie die in der PGVO erwähnten Voraussetzungen (Rechteverwaltung, Löschfristen) sowie die darüber hinaus allgemein gültigen Anforderungen (v.a. in Bezug auf Informationssicherheit) in technischer und organisatorischer Hinsicht umgesetzt wurden. Aus diesem Grund beauftragte die Datenschutzstelle die Fachstelle Informationssicherheit der Dienstabteilung Organisation und Informatik der Stadt Zürich (OIZ) mit einer diesbezüglichen Überprüfung des Datensystems MIDA. Diese Überprüfung ergab, dass die sicherheitsrelevanten Informationen zu MIDA nicht in ausreichendem Masse dokumentiert waren. Nicht vorhanden waren insbesondere ein Informationssicherheits- und Datenschutzkonzept sowie ein Rollen- und Berechtigungskonzept. Die Überprüfung ist noch nicht abgeschlossen. In einem Zwischenbericht zuhanden der Datenschutzstelle hält die Fachstelle Informationssicherheit fest, dass die Stadtpolizei das Datensystem MIDA unter guter Kontrolle hat, der Umgang mit den sensitiven Daten mit der nötigen Sorgfalt erfolgt und die erwähnten Konzepte zwischenzeitlich erstellt worden sind. Die Konzepte werden nach deren Finalisierung der Datenschutzstelle zugestellt. Ausstehend ist insbesondere noch die technische Sicherstellung, dass die Daten nach fünf Jahren gelöscht werden. Bis dahin gehört die Gewährleistung dieser Anforderung zu den regelmässigen Aufgaben des Systemadministrators.

4 Auskunft über Daten der Stadtpolizei

«Jede Person hat Anspruch auf Zugang zu den eigenen Personendaten.» Die Umsetzung dieses Rechts nach Informations- und Datenschutzgesetz des Kantons Zürich (IDG) hat die Stadtpolizei in Zusammenarbeit mit der Datenschutzstelle grundlegend geprüft und neu konzipiert.

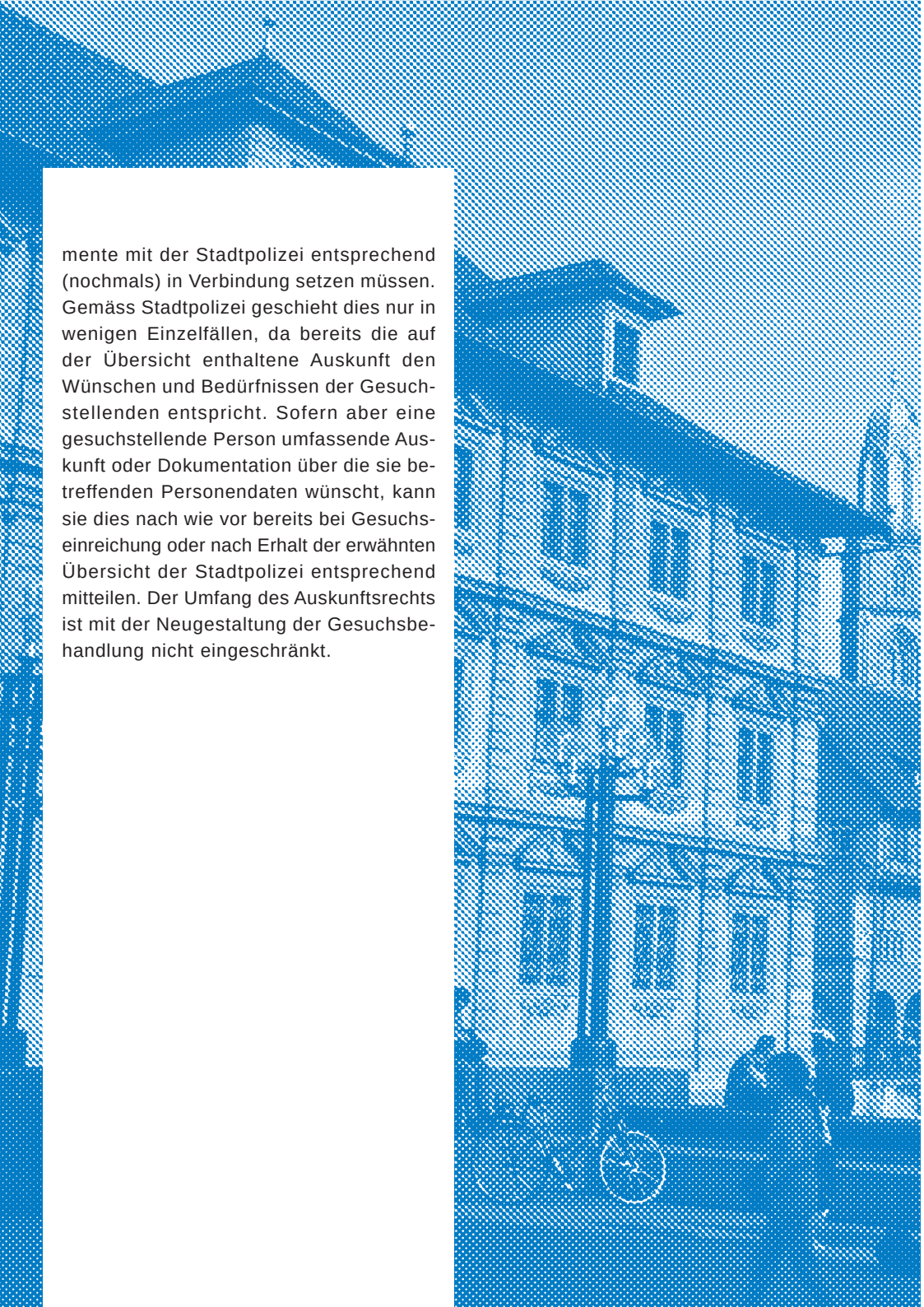
Bevor auf diesen Anspruch gemäss IDG näher eingegangen werden kann, muss erst einmal klargestellt werden, was er nicht ist. Abzugrenzen ist dieses Recht insbesondere von den Gesuchen um Akteneinsicht, die Strafverfahren betreffen. Da für die Durchführung von Strafverfahren die Staatsanwaltschaft zuständig ist, hat auch sie nach den massgebenden Regeln der Schweizerischen Strafprozessordnung (StPO) über Einsicht in die Verfahrensakten zu entscheiden. Dies gilt auch für die Akten, die die Stadtpolizei gestützt auf die StPO erstellt und an die Staatsanwaltschaft weiterleitet. Gesuche um Akteneinsicht, die Strafverfahren betreffen, werden deshalb von der Polizei an die Staatsanwaltschaft weitergeleitet oder erst nach Rücksprache mit dieser behandelt. Derartige Gesuche von Beteiligten an Strafverfahren sowie die Gesuche von Versicherungen, die für die Klärung von Haftungsansprüchen auf die Herausgabe von Akten angewiesen sind, stellen das eigentliche Tagesgeschäft dar, mit welchem sich das Büro für Akteneinsicht der Stadtpolizei hauptsächlich beschäftigt.

Vom Recht auf Akteneinsicht bei Strafverfahren ist das datenschutzrechtliche Zugangs- bzw. Auskunftsrecht nach IDG zu unterscheiden. Dieses Auskunftsrecht kann in gewissen Fällen zwar eine (inhaltliche) Überschneidung zur verfahrensrechtlichen Akteneinsicht darstellen, unterscheidet sich aber dennoch von dieser in mehrfacher Hinsicht. Das Zugangs- bzw. Auskunftsrecht nach IDG besteht grundsätzlich voraussetzungslos und unabhängig von einem (förmlichen) Verfahren gegenüber jeder Verwaltungsstelle, die Personendaten bearbeitet. Materiell ist der Anspruch aber eingeschränkt auf Zugang zu bzw. Auskunft über eigene Personendaten. Wie jedes Recht gilt auch dieser Anspruch nicht absolut. Der Zugang zu eigenen Personen ist zu verweigern oder einzuschränken, wenn überwiegende öffentliche oder private Interessen entgegenstehen.

Die Fallzahlen zeigen, dass auch dieses allgemeine Auskunftsrecht nach IDG bei der Stadtpolizei zunehmend an Bedeutung gewinnt. Waren es in den Jahren 2011 und 2012 noch circa 40 Personen pro Jahr, die von der Stadtpolizei gestützt auf das IDG Auskunft über die sie betreffenden Daten wünschten, waren es im Jahr 2013 bereits über 60 Personen und für das Jahr 2014 kann (hochgerechnet) von ca. 80 Personen ausgegangen werden. Grund genug also, dass auf eine korrekte Umsetzung dieses Auskunftsrechts Wert gelegt wird und hierfür die internen Abläufe und die Kommunikation mit den Gesuchstellenden überprüft und wo nötig angepasst wurden.

Auf der Webseite informiert die Stadtpolizei heute kurz und verständlich, in welcher Weise das Auskunftsrecht über eigene Personendaten geltend gemacht werden kann und stellt hierfür ein Formular zur Verfügung. Gleichzeitig informiert die Stadtpolizei, dass Personendaten in vier Informationsbeständen bearbeitet werden, nämlich in der POLIS-Datenbank, der Milieu-Datenbank, der Lärmkartei sowie einem Bewilligungsregister. Auf dem Formular kann durch Ankreuzen angegeben werden, über welche dieser Informationsbestände Auskunft gewünscht wird. Mit dem standardisierten Antwortschreiben informiert die Stadtpolizei die Gesuchstellenden anschliessend in einem ersten Schritt, welche Einträge zu ihrer Person in den Informationsbeständen vorhanden sind. Dies erfolgt in einer Übersichtsform, gegliedert nach Datum/Ereignis/Örtlichkeit und unter Angabe, in welcher Beteiligungsform (bspw. Geschädigter, Beschuldigter, Auskunftsperson) die gesuchstellende Person registriert ist. Dabei wird – auch durch entsprechend klare Gestaltung der Übersicht – unterschieden, ob es sich um Akten handelt, die zum Zeitpunkt der Gesuchseinreichung im Zuständigkeitsbereich der Stadtpolizei liegen oder ob es sich um Akten handelt, die an andere Behörden (Staatsanwaltschaft/Stadtrichteramt) weitergeleitet wurden. Für Auskünfte zu weitergeleiteten Akten werden die Gesuchstellenden auf die jeweils angegebenen Behörden verwiesen. Wünschen Gesuchstellende weitergehende Auskünfte oder Kopien von Dokumenten zu Einträgen, die im Zuständigkeitsbereich der Stadtpolizei liegen, werden sie an das Büro für Akteneinsicht der Stadtpolizei verwiesen, welches diese Wünsche auch telefonisch entgegen nimmt. Am Schluss des standardisierten Antwortschreibens bestätigt die Stadtpolizei den Gesuchstellenden ausdrücklich, dass diese in keinen weiteren von der Stadtpolizei geführten Informationsbeständen verzeichnet sind.

Das Auskunftsrecht nach IDG bezieht sich grundsätzlich auf alle Personendaten, die bei einer angefragten Verwaltungsstelle über eine gesuchstellende Person bearbeitet werden. Gemäss Angaben der Stadtpolizei wünschen jedoch die weitaus meisten Gesuchstellenden nicht eine uneingeschränkte Auskunft, die alle sie betreffenden Personendaten umfasst. Vielmehr werde fast immer nur eine gezielte Auskunft gewünscht, die nur bestimmte Informationsbestände oder nur bestimmte Vorfälle betrifft. Aus diesem Grunde und in Berücksichtigung des nicht unerheblichen Aufwandes, der mit Auskunftsgesuchen verbunden sein kann, ist es nach Ansicht der Datenschutzstelle gerechtfertigt, das Auskunftsrecht bei der Stadtpolizei nicht nach dem Giesskannenprinzip auszugestalten. So macht es Sinn, bereits von Beginn an, d.h. auf dem von der Stadtpolizei zur Verfügung gestellten Formular, die Möglichkeit zur Einschränkung auf nur bestimmte Informationsbestände vorzusehen. Auch ist es verhältnismässig, dass die Gesuchstellenden in einem ersten Schritt nur die erwähnte Übersicht erhalten und sich für weitergehende Auskünfte oder Doku-



mente mit der Stadtpolizei entsprechend (nochmals) in Verbindung setzen müssen. Gemäss Stadtpolizei geschieht dies nur in wenigen Einzelfällen, da bereits die auf der Übersicht enthaltene Auskunft den Wünschen und Bedürfnissen der Gesuchstellenden entspricht. Sofern aber eine gesuchstellende Person umfassende Auskunft oder Dokumentation über die sie betreffenden Personendaten wünscht, kann sie dies nach wie vor bereits bei Gesuchseinreichung oder nach Erhalt der erwähnten Übersicht der Stadtpolizei entsprechend mitteilen. Der Umfang des Auskunftsrechts ist mit der Neugestaltung der Gesuchsbehandlung nicht eingeschränkt.

5 Abrechnung medizinischer Leistungen bei der Ausnüchterungsstelle

Wer eine Nacht in der Ausnüchterungsstelle der Stadt verbrachte, kam bisher nicht darum herum, dies seiner Krankenversicherung offen zu legen. Die Städtischen Gesundheitsdienste haben diese Praxis nach Intervention der Ombuds- und Datenschutzstelle angepasst.

Die gängigen Diskussionen im Bereich der obligatorischen Krankenversicherungen drehen sich oft um das Thema der Kosten: Werden die medizinischen Leistungen übernommen oder nicht? Welche Tarife gelten? Datenschutzrechtlicher Streitpunkt ist dabei immer wieder die Frage, welche Patienteninformationen für die gesetzlich vorgesehene Überprüfung der Zweckmässigkeit und Wirtschaftlichkeit einer Behandlung die Krankenversicherer herausverlangen können. Dabei werden die Informationsansprüche der Krankenversicherer jeweils mit den Ansprüchen auf Schutz der Privatsphäre der Patientinnen und Patienten gegeneinander abgewogen und je nach Interessen unterschiedlich gewichtet. Ausser Diskussion steht in der Regel, dass eine Krankenversicherung nur dann die Kosten für eine Leistung zu übernehmen hat, wenn sie eine detaillierte und verständliche Rechnung erhält. Solche Rechnungen enthalten neben rein administrativen Angaben zum Teil auch sehr sensible medizinische Informationen. Patientinnen und Patienten können deshalb verlangen, dass die medizinischen Informationen nur dem Vertrauensarzt der Versicherung übermittelt werden. Dass bereits die Bekanntgabe von administrativen Informationen an den Krankenversicherer bei einer Bagatellrechnung von CHF 90 heikel sein kann, hat ein Praxisfall der Ombudsstelle, für dessen Klärung die Datenschutzstelle im Berichtsjahr involviert wurde, gezeigt:

Seit rund zwei Jahren kann die Polizei Personen, welche aufgrund übermässigen Alkoholkonsums sich selber oder Dritte gefährden, in die Zentrale Ausnüchterungsstelle (ZAS+) einweisen, wo sie medizinisch überwacht und versorgt werden. Für die medizinische Überwachung und Pflege sind die Städtischen Gesundheitsdienste (SGD) zuständig. Der von den SGD mit den Krankenversicherungen in einem Tarifvertrag mit Santé Suisse vereinbarte Pauschalbetrag für die medizinische Versorgung beträgt dabei pro Person und Tag CHF 90. Mit diesem Betrag sind alle medizinischen Leistungen abgegolten, weshalb auf eine Detailabrechnung einzelner Leistungen und den damit verbundenen administrativen Aufwand verzichtet werden kann. In den Tarifverträgen werden in aller Regel nicht nur die Kostenbeiträge, sondern auch der jeweilige Abrechnungsmodus vereinbart. Unterschieden wird zwischen den beiden Abrechnungsmodi Tier Garant und Tier Payant. Beim Tier Garant, welcher üblicherweise im ambulanten Bereich zur Anwendung kommt, stellt der Leistungserbringer die Rechnung der Patientin bzw. dem Patienten zur direkten Zahlung zu. Die Krankenversicherung vergütet dann die bezahlte Rechnung an ihre Versicher-

ten zurück. Demgegenüber erfolgt beim Tier Payant die Rechnungsstellung der Leistungserbringer direkt an die Krankenversicherung. Die versicherten Patientinnen und Patienten erhalten jeweils erst im Nachhinein eine Rechnungskopie. Je nach Höhe der Franchise fordern die Krankenversicherungen die von ihr bezahlten Rechnungen bei den Versicherten wieder ein. Gestützt auf das vereinbarte Abrechnungsverfahren des Tier Payant bei der ZAS+ stellte die SGD den Krankenversicherungen jeweils eine Rechnung mit dem Vermerk «Zentrale Ausnüchterungsstelle» zu. Für die Krankenversicherer war damit ohne Weiteres ersichtlich, dass ihre Versicherten in die ZAS+ eingeliefert wurden.

Die Datenschutzstelle erachtete die Anwendung des Tier Payant im Falle der ZAS+ als heikel. Für die Abgeltung des Pauschalbetrags von CHF 90 hatte ein Patient oder eine Patientin in Kauf zu nehmen, dass der Krankenversicherung die Behandlung in der ZAS+ bekannt wurde. Besonders stossend kann dies in Fällen hoher Franchisen sein: Systembedingt durch die Anwendung des Tier Payant kann es dazu kommen, dass die Krankenversicherer vom Leistungserbringer zwar die Rechnungsinformationen erhalten, ohne aber letztlich für die Leistungen aufkommen zu müssen.

Ein Schutz des Patientengeheimnisses gegenüber der Krankenversicherung kann nur dann erreicht werden, wenn Patientinnen oder Patienten auf die Inanspruchnahme der Krankenversicherung verzichten. Im Abrechnungsmodus des Tier Garant liegt dieser Entscheid automatisch in der Hand der Patientinnen und Patienten, da sie selber Rechnungsempfänger sind und dadurch selber entscheiden können, ob sie eine Rückerstattung bei ihrer Krankenversicherung verlangen oder nicht. Eine solche Möglichkeit ist im System des Tier Payant eben gerade nicht vorgesehen.

Im Falle der ZAS+ ist die Datenschutzstelle zur Beurteilung gelangt, dass Patienten und Patientinnen die Möglichkeit gewährt werden sollte, auf die Inanspruchnahme der Krankenversicherung zu verzichten und dadurch zu verhindern, dass diese vom Aufenthalt in der ZAS+ erfährt. Die Datenschutzstelle hat aus diesen Gründen den SGD empfohlen, die betroffenen Patientinnen und Patienten beim Austritt über die Abrechnung im Tier Payant zu informieren und ihnen gleichzeitig die Möglichkeit zu geben, den Pauschalbetrag von CHF 90 selber zu bezahlen. Ausserdem hat die Datenschutzstelle empfohlen, die Adressierungsinformationen auf der Rechnung zuhanden der Krankenversicherungen so anzupassen, dass keine stigmatisierenden Informationen wie «Zentrale Ausnüchterungsstelle» mehr enthalten sind.

Beiden Empfehlungen sind die SGD nachgekommen. Neu werden die Betroffenen beim Austritt über das Abrechnungsverfahren informiert. Sie können dabei wählen, ob der Betrag direkt mit der Krankenversicherung abgerechnet werden soll oder sie den Betrag selber bezahlen und allenfalls bei ihrem Krankenversicherer rückvergüten lassen wollen. Die Rechnungsinformationen wurden so angepasst, dass im Absender nur noch die SGD aufgeführt sind.

6 Kommunale Pflegefinanzierung

Seit der Neuregelung der Pflegefinanzierung müssen die Gemeinden Pflegekosten direkt übernehmen. Damit die Abrechnungen der Pflegebeiträge kontrolliert werden können, werden Informationen mit den Krankenkassen ausgetauscht und Pflegebedarfsermittlungen stichprobenweise überprüft.

Seit dem 1. Januar 2011 ist das kantonale Pflegegesetz in Kraft, welches die Pflegefinanzierung auf der Grundlage des Bundesgesetzes über die Krankenversicherung (KVG) neu regelt. Die Finanzierung der ambulanten Pflege (Spitex) und der stationären Pflege (Alters- oder Pflegeheime) wird auf drei Träger verteilt: Krankenversicherung, pflegebedürftige Person und öffentliche Hand. Die ausgewiesenen Pflegekosten, die nach Abzug der Krankenkassenbeteiligung und des Eigenanteils der pflegebedürftigen Personen noch nicht gedeckt sind, werden im Rahmen des kantonalen Pflegegesetzes von der öffentlichen Hand übernommen. Die Kostenbeteiligung der öffentlichen Hand stützt sich dabei auf die von den Krankenversicherungen anerkannten Rechnungen, welche von den Leistungserbringern auf Basis des Pflegebedarfs gemäss KVG gestellt werden. Die Gemeinden haben daher ein berechtigtes Interesse an der Kontrolle der korrekten Rechnungsstellung und der zu Grunde liegenden Pflegebedarfsermittlung. Dies setzt einen entsprechenden Informationsaustausch zwischen den Leistungserbringern, den Krankenversicherungen und den Gemeinden voraus. Dieses Thema hat im Berichtsjahr auch die Datenschutzstelle beschäftigt, wie die folgenden Vorhaben des Städtischen Amtes für Zusatzleistungen (AZL) und der Städtischen Gesundheitsdienste (SGD) zeigen.

a) Auslagerung des Pflegecontrollings
Die Kontrolle der korrekten Pflegebedarfsermittlung fällt gemäss KVG primär in den Zuständigkeitsbereich der Krankenversicherungen. Gestützt auf das kantonale Pflegegesetz können aber auch die Gemeinden (als beteiligte Kostenträger) stichprobenweise den Pflegebedarf einzelner Patientinnen und Patienten überprüfen und entsprechende Anpassungen veranlassen. Für die Überprüfung des Pflegebedarfs ist in der Regel die Einsichtnahme in das Pflegedossier und damit in sensible Patienteninformationen notwendig. Das Amt für Zusatzleistungen (AZL), welches für die Zahlung der Beiträge im stationären Pflegebereich (Alters- und Pflegeheime) zuständig ist, hat im Berichtsjahr eine spezialisierte Krankenversicherung mit dem Controlling der Bedarfsabklärungen beauftragt. Die Möglichkeit zur Auslagerung des Pflegecontrollings ist sowohl gemäss kantonalem Pflegegesetz als auch gestützt auf das IDG grundsätzlich zulässig. Verlangt wird eine vertragliche Vereinbarung, in welcher der Auftrag klar geregelt ist und der Umgang mit Personendaten, die Geheimhaltungsverpflichtungen und die zum Schutz der Informationen vorzukehrenden Massnahmen verbindlich festgehalten sind.

Die Datenschutzstelle hat das AZL fachlich unterstützt und die mit der beauftragten Krankenversicherung getroffenen vertraglichen Regelungen überprüft. Dabei wurde ein besonderes Augenmerk darauf gelegt, dass

- der Auftrag, die damit verbundenen Rollen des AZL als Auftraggeberin und der Krankenversicherung als Auftragnehmerin sowie die Datenbearbeitungen genau definiert sind;
- die Auswahl der zu kontrollierenden Alters- und Pflegeheime als Stichproben erfolgen und der Auswahlprozess klar geregelt ist;
- keine Dossiers, bei welchen die Auftragnehmerin selber Versicherungsleistungen erbringt, im Auftrag und auf Kosten der Stadt Zürich durch die Auftragnehmerin kontrolliert werden;
- nur vor Ort Einsicht in die Pflegedossiers genommen werden darf und nur die Kontrollergebnisse durch die Auftragnehmerin im Kontrollbericht festgehalten und an das AZL weitergeleitet werden dürfen;
- die Geheimhaltungsverpflichtungen geregelt sind.

Die Auslagerung des Pflegecontrollings bietet aus datenschutzrechtlicher Optik den Vorteil, dass das AZL selber keinen Einblick in die sensiblen Pflegedossiers hat, womit die Privatsphäre der Betroffenen gegenüber der administrativen Stadtverwaltung weitestgehend geschützt wird.

b) Abgleich von Rechnungsdaten
Leistungskürzungen der Krankenversicherungen haben entsprechende Beitragskürzungen der öffentlichen Hand zur Folge. Die Spitexorganisationen müssen daher den Gemeinden allfällige Leistungskürzungen bzw. Kürzung der Pflegestunden melden. Dies klappt in der Praxis nicht immer reibungslos. Die Städtischen Gesundheitsdienste (SGD), welche für die Zahlung der Pflegebeiträge an die Spitexorganisationen in der Stadt Zürich zuständig sind, haben deshalb zusammen mit Vertretern einzelner Krankenversicherungen nach einer entsprechenden Kontrollmöglichkeit gesucht. Als Lösungsvariante wurde seitens der Krankenversicherungen in Betracht gezogen, den SGD jeweils die Kostengutspracheentscheide zuzustellen, aus welchen die anerkannten Pflegestunden ersichtlich sind. Insbesondere negative Kostengutspracheentscheide können aber in den Begründungen sehr sensible Patienteninformationen enthalten. Dadurch hätten die SGD sensible Patienteninformationen erhalten, welche für den bezweckten Rechnungsabgleich bzw. den Abgleich der Pflegestunden gar nicht notwendig sind. Sowohl die SGD als auch die Krankenversicherungen haben diese Datenschutzproblematik erkannt und als Alternative für den Rechnungsabgleich bzw. den Abgleich der Pflegestunden den folgenden Informationsaustausch vorgesehen:

Die SGD stellen den jeweiligen Krankenversicherungen im monatlichen Turnus Listen der Versicherten zu, auf welchen die

von der Spitex in Rechnung gestellten Pflegestunden vermerkt sind. Die Krankenversicherungen ergänzen diese Listen mit den effektiv anerkannten Pflegestunden und retournieren diese den SGD. Durch diesen einfachen Informationsaustausch können allfällige Abrechnungsdifferenzen leicht erkannt und die Rechnungen korrigiert werden. Dieses Kontrollverfahren wird bei kleineren Spitexorganisationen angewandt, mit welchen die SGD keine Leistungsvereinbarungen abgeschlossen haben.

Die Datenschutzstelle hat auf Anfrage der SGD die Zulässigkeit dieses Informationsaustausches überprüft. Dabei ist die Datenschutzstelle zum Ergebnis gekommen, dass der gegenseitige Informationsaustausch zwischen den SGD und den Krankenversicherungen auf das Krankenversicherungsgesetz (KVG) abgestützt werden kann. Dieses ermächtigt Organe, welche an der Durchführung und der Kontrolle der obligatorischen Krankenversicherung beteiligt sind, die für die Aufgabenerfüllung notwendigen Informationen bzw. Personendaten auszutauschen. Aufgrund der gesetzlichen Pflicht der Gemeinden zur Restfinanzierung von Pflegeleistungen ist davon auszugehen, dass den SGD Organstellung im Sinne des KVG zukommt. Die Datenschutzstelle konnte zudem feststellen, dass nur die für die Abrechnungskontrolle notwendigen Informationen ausgetauscht werden und damit die Verhältnismässigkeit des Datenaustausches gewahrt ist. Insbesondere erhalten die Krankenversicherungen keine (zusätzlichen) Informationen, über welche sie nicht bereits verfügen. Da mit diesem Datenabgleich auf die Zustellung der sensiblen Kostengutspracheentscheide verzichtet werden kann, trägt das von den SGD und den beteiligten Krankenversicherungen umgesetzte Kontrollverfahren wesentlich zum Schutz der Privatsphäre der pflegebedürftigen Patientinnen und Patienten bei.

7 Datenschutz-Richtlinie für Spitexorganisationen

Spitexorganisationen müssen auch in Sachen Datenschutz und Informationssicherheit fit sein. Helfen soll dabei eine neue Richtlinie des kantonalen Spitexverbands.

Für die Spitexorganisationen des Kantons Bern hat der bernische Spitexverband in Absprache mit dem Datenschutzbeauftragten sowie der Gesundheits- und Fürsorgebehörde des Kantons Bern die wichtigsten datenschutzrechtlichen Themen in Form von Spitexrichtlinien geregelt. In Anlehnung an diese Richtlinien hat der Spitexverband des Kantons Zürich die Ausarbeitung entsprechender Richtlinien für die zürcherischen Spitexorganisationen veranlasst. Unter der Federführung des kantonalen Datenschutzbeauftragten wurde zusammen mit Vertreterinnen und Vertretern des kantonalen Spitexverbandes, der Direktorin der städtischen Spitexorganisation Limmat sowie unter Mitwirkung der städtischen Datenschutzstelle die Ausarbeitung einer Richtline an die Hand genommen. Dabei mussten zahlreiche fachliche und rechtliche Fragen im Rahmen von Vorabklärungen mit den involvierten Vertreterinnen und Vertretern sowie der kantonalen Gesundheitsdirektion geklärt werden. Die erarbeiteten Spitexrichtlinien richten sich an die kantonalen und städtischen Spitexorganisationen und geben einen Überblick über die wichtigsten datenschutzrechtlichen Themen im Bereich Spitex:

- Rechtliche Grundlagen im Bereich Spitex;
- Aufbewahrung, Verwaltung, Löschung und Archivierung von Klienteninformationen;
- Schweigepflichten im Bereich Spitex;
- Informationsaustausch zwischen Arzt und Spitex;
- Informationsaustausch zwischen Spitex, Sozial- und Privatversicherungen;
- Herausgabe von Daten und Dokumenten an Familienangehörige, Bezugspersonen, Medizinalpersonen ausserhalb der Spitexorganisation;
- Melderechte und Meldepflichten gegen über der Kindes- und Erwachsenenschutzbehörde;
- Wichtige Grundsätze im Bereich der Informationssicherheit.

Aufgrund der organisatorischen Unterschiede der Spitexinstitutionen mussten die Richtlinien zum Teil sehr allgemein gehalten werden. Wichtige datenschutzrechtliche Themen werden aber dennoch mindestens in den Grundzügen beschrieben. Diese geben den Spitexinstitutionen wichtige Grundlageninformationen für die Umsetzung der rechtlichen Vorgaben innerhalb ihrer eigenen Organisation.

8 Meldung von Informationen zu Sozialhilfebeziehenden an Krankenversicherungen

Krankenkassenprämien sind nicht mehr von den Sozialhilfebeziehenden, sondern direkt von den Gemeinden zu bezahlen. Dieser Wechsel zur Direktüberweisung hat auch Konsequenzen für den Informationsaustausch zwischen den Sozialen Diensten der Stadt Zürich und den Krankenversicherungen

Seit dem 1. Januar 2014 müssen die Gemeinden die Krankenversicherungsprämien sozialhilfeberechtigter Personen direkt an die Krankenversicherungen überweisen. Die Sozialämter können seither den Sozialhilfebezügerinnen und -bezügern nicht mehr erlauben, die Krankenkassenprämien, die nicht durch die Prämienverbilligung gedeckt sind, aus der gewährten Sozialhilfe selber an ihre jeweiligen Krankenversicherungen zu bezahlen – so wie dies früher der Praxis der Stadt Zürich entsprach. Seit der Revision des kantonalen Einführungsgesetzes zum Krankenversicherungsgesetz (EG KVG) gehen die Prämienforderungen der Krankenkassen von Gesetzes wegen auf die Gemeinden über, d.h. Prämienschuldnerin gegenüber den Versicherungen ist nun die Gemeinde.

Im Berichtsjahr gelangte die Dienstabteilung Soziale Dienste (SOD) an die Datenschutzstelle mit der Frage, ob im Hinblick auf die praktische Umsetzung der gesetzlich verlangten Direktüberweisungen den Krankenversicherungen die versicherten Sozialhilfebezügerinnen und -bezüger gemeldet werden dürfen, bei welchen die Stadt Zürich die Prämien im Sinne des EG KVG übernimmt bzw. Prämienschuldnerin ist.

Die Datenschutzstelle hat diese Frage abgeklärt und gegenüber den SOD die Ansicht vertreten, dass für die Umsetzung der gesetzlich verlangten Direktüberweisung die Krankenversicherer wissen müssen, für welche Klientinnen und Klienten die Gemeinden die Prämien ab einem bestimmten Zeitpunkt übernehmen. Dies setzt voraus, dass die Stadt Zürich bzw. die SOD den jeweiligen Krankenversicherungen vorgängig diejenigen Personendaten der Sozialhilfebeziehenden, welche zu deren Identifizierung erforderlich sind, bekannt gibt. Mit den revidierten Regelungen im EG KVG bestehen nach Ansicht der Datenschutzstelle ausreichende Rechtsgrundlagen für diese Datenbekanntgaben bzw. Meldungen – auch wenn die einzelnen bekannt zu gebenden Daten nicht ausdrücklich im Gesetz genannt sind.

Aufgrund des Systemwechsels ist die Stadt Zürich neu Prämienschuldnerin von circa 11'000 Personen. Nicht tangiert von diesem Systemwechsel ist die Rechnungsstellung für medizinische Leistungen. Diesbezügliche Rechnungen gehen nach wie vor an den Versicherten selber. Das Patientengeheimnis bleibt gewahrt.

9 Zugriffs- und Berechtigungskonzepte

Zugriffs- und Berechtigungskonzepte sind zentrale Instrumente bei der Umsetzung des Verhältnismässigkeitsgrundsatzes und der Informationssicherheit. Die Datenschutzstelle hat sich vertieft mit dem Thema auseinandergesetzt und zusammen mit der städtischen Fachstelle für Informationssicherheit Mustervorlagen ausgearbeitet. Diese sollen bei Informatikprojekten in der Stadtverwaltung zu einem einheitlichen, datenschutzkonformen Qualitätsstandard beitragen.

Zum Standard bei den Informatikprojekten der Stadtverwaltung gehört das Erstellen eines Informationssicherheits- und Datenschutz-Konzepts. Als Teil dieses ISDS-Konzepts müssen die Projektverantwortlichen auch ein sog. Zugriffs- und Berechtigungskonzept verfassen. Wie die Datenschutzstelle im Praxisalltag regelmässig feststellt, sind die Vorstellungen der Projektverantwortlichen hinsichtlich Inhalt, Umfang, Form und Detaillierungsgrad eines Zugriffs- und Berechtigungskonzepts sehr unterschiedlich. Dies dürfte vor allem darauf zurückzuführen sein, dass in der Stadt Zürich diesbezüglich bisher keine einheitlichen Vorgaben und Vorlagen bestanden. Die Datenschutzstelle hat sich im Berichtsjahr vertieft mit dem Thema «Zugriffs- und Berechtigungskonzept» auseinandergesetzt und zusammen mit der Fachstelle Informationssicherheit der Dienstabteilung Organisation und Informatik (OIZ) Mustervorlagen ausgearbeitet und die entsprechenden Anforderungen in einer Wegleitung beschrieben.

Zugriffs- und Berechtigungskonzepte sind wichtige Instrumente bei der Umsetzung des im Datenschutzrecht geltenden Verhältnismässigkeitsgrundsatzes. Dieser verlangt, dass die Zugriffsberechtigungen auf das für die gesetzliche Aufgabenerfüllung notwendige Mass beschränkt werden. Um dieses (notwendige) Mass finden zu können, müssen sich die Projektverantwortlichen vertieft mit den systemrelevanten Geschäftsprozessen auseinandersetzen. Erst wenn diese Auseinandersetzung erfolgt ist, können die einzelnen Rollen mit den damit verbundenen Berechtigungen und die Nutzungsgruppen bestimmt werden. Dies ist primär Aufgabe der für die einzelnen Geschäftsprozesse verantwortlichen Stellen und Fachpersonen. Die Datenschutzstelle stellt bei Projekten immer wieder fest, dass diese Aufgabe (zumindest) teilweise an die Lieferanten von Systemen oder Applikationen bzw. die Technik delegiert wird. Neben der Umsetzung des Verhältnismässigkeitsgrundsatzes haben Zugriffs- und Berechtigungskonzepte aber auch eine wichtige organisatorische und technische Funktion, bspw. hinsichtlich Regelung der Verantwortlichkeiten oder als Grundlage für die Parametrisierung der Systeme. Die erstellte Mustervorlage beinhaltet die wichtigsten Themen, welche gestützt auf das Datenschutzrecht und das städtische Handbuch für Informationssicherheit in einem Zugriffs- und Berechtigungskonzept beschrieben und geregelt werden müssen. Die Vorlage des Zugriffs- und Berechtigungskonzepts wurde in Form einer elektronischen Excel-Matrix erstellt, in welcher für jedes einzelne Rollenprofil unter anderem die folgenden Themen beschrieben werden:

- Rollen: Rollenbezeichnung, mit der Rolle verbundene Geschäftsprozesse, nutzungsberechtigte Abteilungen und Funktionsträger;
- Prozesse: Benutzerverwaltung, Authentisierungs- und Registrierungsverfahren, Änderung und Löschung von Berechtigungen, Dokumentation, Historisierung;
- Objekte: Beschrieb der mit einer Rolle verbundenen Systeme, Anwendungen und Daten;
- Berechtigungen: Lese-, Änderungs- oder Löschungsrecht;
- Verantwortung: Erstellung, Aktualisierung und Änderung von Rollen;
- Kontrolle: Verhältnismässigkeitsprüfung und Prüfung besonderer Geheimhaltungsbestimmungen.

Neben diesen rollenbezogenen Themen werden auch allgemeine systembezogene Themen beschrieben, wie bspw. die Überwachung (Monitoring) der Zugangsberechtigungen (Logging der Aktivitäten; Auswertung der Logfiles).

Zugriffs- und Berechtigungskonzepte sind als Teil des ISDS-Konzepts grundsätzlich auch Gegenstand der Vorabkontrolle durch die Datenschutzstelle. Die Erarbeitung solcher Konzepte kann aber in der Regel erst in der Implementierungsphase eines Informatikprojekts erfolgen (so auch gemäss der in der Stadtverwaltung verbindlichen Projektführungsmethode HERMES), so dass im Zeitpunkt der Vorabkontrolle noch keine vollständigen und detaillierten Zugriffs- und Berechtigungskonzepte vorliegen können. Gestützt auf das Datenschutzrecht wird dies denn auch nicht verlangt: Im Rahmen einer Vorabkontrolle sind grundsätzlich nur die rechtlichen, organisatorischen und technischen Rahmenbedingungen und keine Detailregelungen zu überprüfen. Bei der Prüfung der Zugriffs- und Berechtigungsregelungen sieht die Datenschutzstelle ihre Kontrollaufgabe vorwiegend darin, sicherzustellen, dass verbindliche und terminierte Projektentscheide bestehen, welche die Ausarbeitung eines datenschutzkonformen Zugriffs- und Berechtigungskonzeptes in nachvollziehbarer Weise garantieren. Nur in Einzelfällen, bei welchen bspw. auf Grund spezialgesetzlicher Geheimhaltungsbestimmungen spezielle Detailanforderungen im Zugriffs- und Berechtigungskonzept zwingend umgesetzt werden müssen und damit als Rahmenbedingung zu betrachten sind, nimmt die Datenschutzstelle eine (weitergehende) Detailprüfung vor. Dies war bspw. der Fall bei der Überprüfung der Zugriffsregelung für die Case-Management-Dossiers, für welche besondere Geheimhaltungsbestimmungen gemäss städtischem Personalrecht gelten.

10 Webstatistik

Globale Internetunternehmen zeigen in der Regel wenig Verständnis für lokale Rechtsordnungen. Die Stadt Zürich konnte dennoch für den Einsatz eines Webstatistik-Tools mit einem internationalen Anbieter eine Vereinbarung abschliessen, die den städtischen Datenschutz- und Informationssicherheitsbestimmungen entspricht.

Für die Optimierung des vielfältigen städtischen Websiteangebots setzt die Stadt Zürich ein Webstatistik-Tool ein. Da dieses nicht mehr den zeitgemässen Anforderungen entspricht und die Bedürfnisse der Stadtverwaltung nicht vollständig zu befriedigen vermag, sucht die Stadtverwaltung seit einiger Zeit eine neue Standardanwendung.

Bereits im Berichtsjahr 2010 hat sich die Datenschutzstelle mit den datenschutzrechtlichen Rahmenbedingungen im Bereich der Webstatistik auseinandergesetzt. Wie im damaligen Tätigkeitsbericht festgehalten wurde, ist die statistische Auswertung der Websitenutzung datenschutzrechtlich grundsätzlich nicht problematisch, sofern bestimmte Voraussetzungen eingehalten werden. Insbesondere muss sichergestellt sein, dass die Daten nur zu statistischen und somit nicht zu personenbezogenen Zwecken bearbeitet werden. Die Personendaten sind sobald als möglich – spätestens nach erfolgter Auswertung – vollständig zu anonymisieren.

Webstatik-Tools erheben und nutzen für die differenzierten Analysen der Websitenutzung in der Regel die Internetprotokoll-Adressen (IP) der Nutzerinnen und Nutzer. In der Rechtsprechung und der Fachliteratur ist heute geklärt, dass mittels IP-Adressen ein Personenbezug hergestellt werden kann und dass daher die damit verbundenen Datenbearbeitungen unter die Datenschutzgesetzgebung fallen. Die gesetzlich verlangte Anonymisierung betrifft daher primär die Anonymisierung der IP-Adressen.

Der Einsatz von Webstatik-Tools bringt in der Regel mit sich, dass wesentliche Datenbearbeitungsprozesse bei der Firma, die das Statistik-Tool anbietet, durchgeführt werden und damit ausserhalb der faktischen Datenherrschaft des Website-Betreibers liegen. Die Datenschutzgesetzgebung verbietet den öffentlichen Organen nicht, Datenbearbeitungen an einen Dritten auszulagern. Vorausgesetzt wird aber, dass die Auftragsdatenbearbeitung in einem schriftlichen Vertrag geregelt und in diesem insbesondere die (für das öffentliche Organ) geltenden Datenschutz- und Informationssicherheitsregelungen der beauftragten Firma überbunden und im Falle eines ausländischen Firmensitzes der Gerichtsstand Zürich vereinbart werden. Diese Voraussetzungen konnten noch vor wenigen Jahren mit dem damals evaluierten Produkt «Google Analytics» nicht erfüllt werden. Die diesbezügliche Prüfung durch die Datenschutzstelle hat ergeben, dass die von der Firma Google einseitig

diktierten Vertragsbestimmungen mit den für die Stadtverwaltung anwendbaren Datenschutz- und Informationssicherheitsbestimmungen nicht vereinbar sind.

Dass ein globales Unternehmen auch andere Wege gehen kann, hat im diesjährigen Berichtsjahr die Firma Adobe bewiesen. Das in der Stadtverwaltung für die Anschaffung eines neuen Webanalyse-Tools eingesetzte Team ist bei Adobe mit ihren Anliegen auf offene Ohren gestossen und konnte einen auf die Stadt Zürich angepassten, individuellen Vertrag aushandeln. Die Datenschutzstelle hat das Projektteam im Vorfeld datenschutzrechtlich beraten und die Vertragsentwürfe überprüft. Sämtliche relevanten Datenschutz- und Informationssicherheitsbestimmungen wurden von Adobe übernommen und die technischen und organisatorischen Schutzmassnahmen werden garantiert. Auswertungen von Informationen der Nutzerinnen und Nutzer städtischer Websites geschehen ausschliesslich nach Massgabe des Auftrags durch die Stadt Zürich. Insbesondere hat sich Adobe dazu verpflichtet, die IP-Adressen nach einem klar definierten, nachvollziehbaren Prozess zu anonymisieren und keine Informationen zu eigenen Zwecken zu nutzen.

11 Datensperre

Die Möglichkeit einer Datensperre ist immer wieder Anlass für Anfragen bei der Datenschutzstelle. Regelmässig müssen dabei Missverständnisse im Zusammenhang mit Umfang sowie Geltungsbereich dieses Rechtsbehelfs geklärt werden.

Namentlich ist den Anfragenden häufig unklar, dass Datensperren nur gegenüber privaten Personen und Organisationen, nicht jedoch gegenüber öffentlichen Organen gelten. In Bezug auf den Austausch von Daten innerhalb der Verwaltung hat die Datensperre keine Wirkung und kann auch nicht verlangt werden. Eine Privatperson kann also mit einer Datensperre den behördeninternen Datenfluss weder verhindern noch einschränken. Ob und inwiefern ein Informationsaustausch bzw. eine Datenbekanntgabe zwischen Verwaltungsbehörden zulässig ist, beurteilt sich nach den rechtlichen Grundlagen des jeweilig einschlägigen Bereichsrechts.

Datensperren kommen nur dann zur Anwendung, wenn Amtsstellen gesetzlich dazu ermächtigt sind, privaten Personen und Organisationen gewisse Daten voraussetzungslos bekanntzugeben. Voraussetzungslose Bekanntgaben sind möglich bei der Einwohnerkontrolle (§ 39 Abs. 1 kantonales Gemeindegesetz), beim Steueramt (§ 122 kantonales Steuergesetz) oder beim Strassenverkehrsamt (Art. 126 Abs. 1 Verkehrszulassungsverordnung des Bundes). Voraussetzungslos heisst insbesondere, dass die um Auskunft ersuchende Person ihr Gesuch nicht begründen, kein Interesse glaubhaft machen oder sogar nachweisen muss. Als Ausgleich dazu muss auch die Person, die eine Datensperre errichten möchte, dies nicht begründen oder sogar ein schutzwürdiges Interesse glaubhaft machen. Jede Person kann von den drei erwähnten Verwaltungsstellen verlangen, dass sie die Bekanntgabe ihrer Personendaten, die von Gesetzes wegen an Private bekannt gegeben werden dürfen, sperren. Die Sperre gilt – wie einleitend erwähnt – nur gegenüber privaten Personen und Organisationen, nicht hingegen gegenüber öffentlichen Organen.

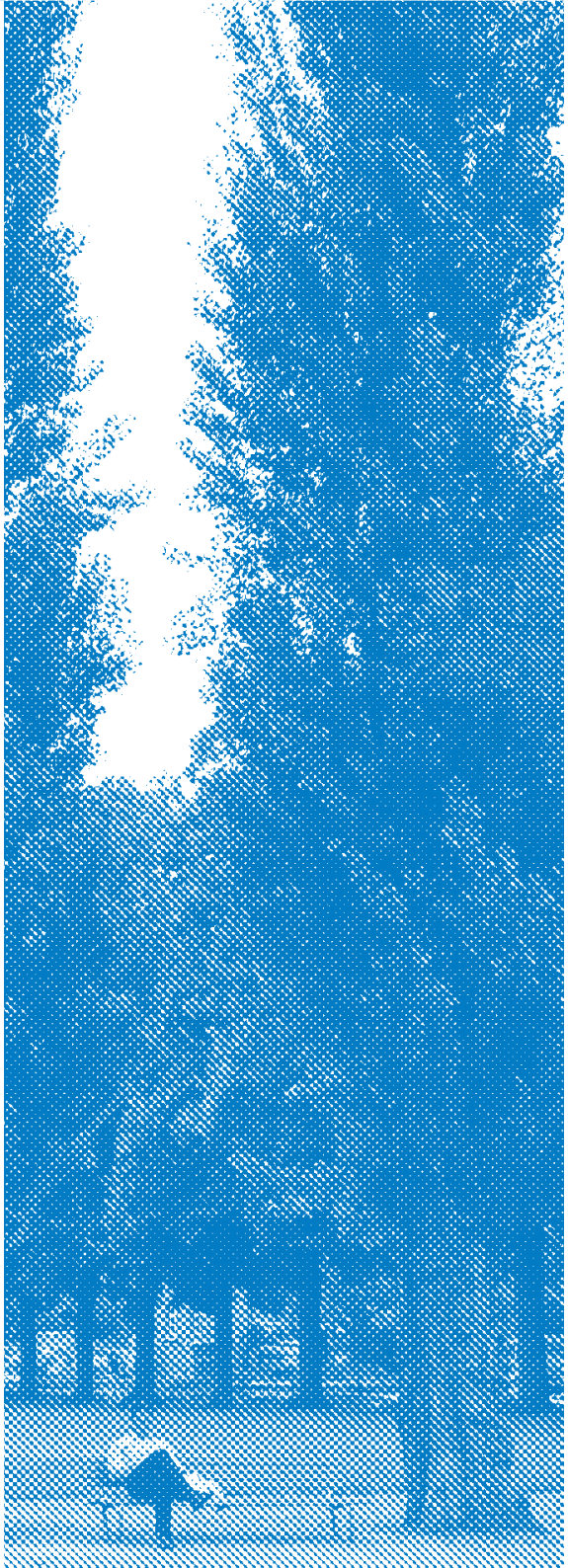
Bei einer Datensperre gestützt auf § 22 IDG handelt es sich um ein Abwehrrecht der betroffenen Person bei an sich zulässigen Bekanntgaben von Personendaten. Obwohl die Datensperre nicht absolut gilt, kann durch diese einer unkontrollierten Datenbekanntgabe an Private entgegengewirkt werden. Die Datensperre stellt ein Recht der Betroffenen dar, welches präventiv zum Zug kommt, also ohne dass eine widerrechtliche Datenbearbeitung vorliegen muss. Eine Sperre kann für eine einzelne Datenbekanntgabe durchbrochen werden, wird jedoch ansonsten nicht berührt. Der (private) Gesuchsteller muss für eine Durchbrechung die zuständige Verwaltungsstelle von der Tatsache überzeugen, dass die Datensperre ihn an der Verfolgung eigener rechtlicher Ansprüche hindert. In der Regel geschieht dies durch Zustellung von Verträgen, Rechnungen oder anderen Dokumenten. Ob der ver-

langte Nachweis im Einzelfall genügt, liegt im pflichtgemässen Ermessen der zuständigen Verwaltungsstelle. Sie kann für die vorzunehmende Interessenabwägung die Person, deren Datensperre durchbrochen werden soll, um Stellungnahme anfragen.

Ein Gesuch um Datensperre muss an jede Amtsstelle separat und schriftlich gerichtet werden. Eine Begründung für die verlangte Datensperre ist nicht notwendig, ebenso wenig bedarf es einer genauen Bezeichnung der zu sperrenden Daten. Die Ausübung des Sperrrechts ist grundsätzlich kostenlos. Um die Ausübung des Sperrrechts zu erleichtern, werden auf den Webseiten der jeweiligen Amtsstellen häufig Musterbriefe zur Verfügung gestellt. Entsprechende Musterbriefe stellen im Kanton bzw. der Stadt Zürich

- das Steueramt (Gesuch um Sperrung der Daten des Steuerregisters www.steueramt.zh.ch),
- das Strassenverkehrsamt (Gesuch um Sperrung der Halterdaten, www.stva.zh.ch) sowie
- das Personenmeldeamt (Gesuch Adress- und Datensperre, www.stadt-zuerich.ch)

zur Verfügung.



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. 044 412 16 00
Fax 044 412 16 10.

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

Quelle Fotos:
Datenschutzbeauftragter der Stadt Zürich
Mediendienste der Stadt Zürich

Gestaltung:
SPUTNIK Vertot, Luzern