Stadt Winterthur

Tätigkeitsbericht 2013

des Datenschutzbeauftragten der Stadt Winterthur

an den Grossen Gemeinderat der Stadt Winterthur

Berichtsperiode vom 1. Januar 2013 bis zum 31. Dezember 2013

Inhaltsverzeichnis

1. Neue Erscheinungsform des Berichts 3

2. Das Berichtsjahr in Kürze 3

3. Schwerpunkt: Videoüberwachung in Winterthur 4

4. Office 365 an Schulen 6

5. Filtrierung der Google-Suche an Schulen 7

6. Schulungen und Vorträge 8

6.1 Schulung der neuen Kaderleute 8

7. Laufende Projekte 8

7.1 Projekt Fokus 9

7.2 Datenbank GREKOS 10

8. Internes 10

8.1 Zwischenrevision der Finanzkontrolle 10

9. Ausblick 11

10. Anhang 13

10.1 Thematische Übersicht 13

10.2 Bearbeitungsstand der Dossiers per 31. Dezember 2013 14

10.3 Aufschlüsselung der Neueingänge nach Aufgaben gemäss § 34 IDG 14

§ 39 Informations- und Datenschutzgesetz des Kantons Zürich (IDG)

Der oder die Beauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkt der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht.

§ 10 Verordnung über den oder die Datenschutzbeauftragte/n der Stadt Winterthur

Der oder die Datenschutzbeauftragte erstattet dem Grossen Gemeinderat jährlich Bericht über seine bzw. ihre Tätigkeit.

1. Neue Erscheinungsform des Berichts

Die bisherigen Tätigkeitsberichte an den Grossen Gemeinderat betreffend die Jahre 2011 respektive 2012 wurden elektronisch sowie in Druckform veröffentlicht. Aus Gründen der Drucklogistik musste die Datenaufsicht stets eine bestimmte Mindestmenge an Exemplaren bestellen, die, wie sich mit der Zeit herausstellte, den tatsächlichen Bedarf des Grossen Gemeinderates sowie der interessierten Öffentlichkeit überstieg. In der Folge können beide Berichte noch immer bei der Datenaufsicht bezogen werden. Schlussendlich werden sie wohl dem Recycling zugeführt.

Als Konsequenz dessen sowie des Umstandes, dass die Fristen der Druckerei stets einen etwas engen Zeitplan zur Folge hatten, beschloss der Datenschutzbeauftragte, den Tätigkeitsbericht nur noch in elektronischer Form zu veröffentlichen.

Im Zuge dieser Neuorientierung wurde das Layout des Tätigkeitsberichts durch die Verwendung einer neuen Schrift sowie Änderung der Zeilenabstände und des Satzspiegels gegenüber den Vorjahren optisch aufgefrischt und für die Darstellung auf Tablets optimiert.[1]

2. Das Berichtsjahr in Kürze

Das Jahr war aus Sicht des Datenschutzbeauftragten insbesondere von einem Wiederanstieg der Fallzahlen geprägt, welche jene des Jahres 2011 noch übertrafen. Eine genaue Aufstellung findet sich im Anhang.

Thematisch stand die Frage der Videoüberwachung klar im Vordergrund, gefolgt von Fragen in Bezug auf Softwareevalutationen, Datenbankdesign, Management und Nutzung von Mobilgeräten, E-Government-Angebote sowie sichere Onlinespeicher für städtische Mitarbeiterinnen und Mitarbeiter.

Neben den Anfragen der städtischen Behörden war wiederum ein leichter Anstieg der Anfragen seitens privater Personen festzustellen. Diese machen mittlerweile rund einen Fünftel der gesamten Anfragen bei der Datenaufsicht aus, was sich jedoch nur bedingt in der Statistik spiegelt, da einige private Anfragen mangels Zuständigkeit an den Eidgenössischen Informations- und Datenschutzbeauftragten weiter verwiesen wurden oder die Datenaufsicht aufgrund des geringen Zeitaufwands der Erledigung kein Dossier eröffnete.

[1] Hinweise bezüglich der Leserlichkeit des Berichts nimmt der Datenschutzbeauftragte gerne über datenaufsicht@win.ch entgegen.

Schliesslich rückt auch der Umzugstermin in den neuen Superblock unaufhaltsam näher. Die Zusammenlegung grosser Teile der Stadtverwaltung in ein einziges Gebäude stellt ein organisatorisches, aber auch ein datenschutzrechtliches Problem dar. Im Vordergrund stehen Fragen der sinnvollen Verteilung von Bereichen der Stadtverwaltung auf die einzelnen Stockwerke, des Umgangs mit Bereichen, die in Bezug auf den Datenschutz strengeren gesetzlichen Regeln unterstehen, des massvollen Umgangs mit technischen Mitteln der Mitarbeiterkontrolle sowie des Datenschutzes am Arbeitsplatz in Grossraumbüros. Eine kurze Übersicht über den derzeitigen Stand findet sich im siebten Abschnitt.

3. Schwerpunkt: Videoüberwachung in Winterthur

Wie bereits in der Jahreszusammenfassung erwähnt, war Videoüberwachung eines der grossen Themen der Berichtsperiode.

Auslöser war eine Initiative der Piratenpartei Winterthur, welche darauf abzielte, sämtliche Überwachungsmassnahmen städtischer Behörden dem Vorbehalt einer Bewilligung durch den Grossen Gemeinderat zu unterstellen. Hierbei stand insbesondere die Überwachung mittels Videoanlagen im Vordergrund.

Die Datenaufsicht wurde zunächst von der Stadtkanzlei angefragt, welche rechtlichen Fragen sich aus Sicht des Datenschutzrechts im Zusammenhang mit einer solchen neuen Prüfungsbefugnis des Parlaments ergäben.

In ihrer Stellungnahme legte die Datenaufsicht dar, dass die vorgesehene Bewilligungsbefugnis sich schwer mit der Rolle des Parlaments im Gefüge der Staatsgewalten vereinbaren liesse. Als Organ der Gesetzgebung sei das Parlament von der politischen Diskussion geprägt. Es eigne sich weniger als Entscheidungsinstanz im Einzelfall, da hier neben Zweckmässigkeitsfragen jeweils rechtliche Überlegungen im Vordergrund stünden, die zum Teil auf Stufe des kantonalen Rechts und des Bundesrechts verbindlich geregelt seien.

Kritisch würde es beispielsweise, wenn eine gesetzlich vorgesehene Überwachung, etwa durch die Stadtpolizei, trotz Erfüllung der gesetzlichen Kriterien keine Bewilligung durch den Grossen Gemeinderat erhielte.

In der Folge beschloss der Stadtrat, eine Videoordnung zu erlassen, welche den Bedenken der Initianten Rechnung tragen sollte. Insbesondere würde die Inbetriebnahme einer Videoanlage zwingend ein Betriebsreglement erfordern, das wiederum der Prüfung der städtischen Datenaufsicht unter-

stünde und nach Erlass in geeigneter Form zu publizieren wäre.

Die neue Videoordnung der Stadt Winterthur trat am 1. September 2013 in Kraft.[2] Die Regelung sah für bestehende Videoanlagen eine Übergangsfrist[3] in Bezug auf den nachträglichen Erlass eines Reglements vor. Entsprechend war die Datenaufsicht im letzten Quartal 2013 vermehrt damit beschäftigt, den städtischen Behörden beim Erlass neuer Überwachungsreglemente beratend zur Seite zu stehen.

In Bezug auf die Publikation erklärte sich der Rechtsdienst der Stadtpolizei bereit, eine entsprechende Webseite im städtischen Internetauftritt aufzubauen und sämtliche Videoreglemente der Stadt zentral zu publizieren.[4] Zudem dienten die Reglemente der Stadtpolizei, die bereits im Sommer vor Inkrafttreten der Videoordnung in Zusammenarbeit mit der Datenaufsicht erlassen worden waren, einigen Stellen in der Stadt als Vorlage, was den Aufwand aller Beteiligten etwas zu senken vermochte.

Es zeigte sich in der Folge, dass gewisse Fragen stets wieder auftauchten und auf ähnliche Weise gelöst werden konnten. Mit der Zeit kristallisierte sich ein gewisser Standard in Bezug auf einige Aspekte der Videoüberwachung heraus.

Beispielsweise wurde entschieden, Bilder von Videoanlagen, deren Aufnahmen dem *alleinigen* Zweck der Beweissicherung in Fällen von Sachbeschädigungen und ähnlichen Straftaten dienen, nicht live auf einen Monitor zu schalten, sondern lediglich zu speichern. Die gespeicherten Daten dürfen sodann nur zur Auswertung im Falle eines Vorfalls[5] verwendet werden, wobei der Entscheid zur Auswertung jeweils nicht von einer Person alleine getroffen wird.

Ausgehend von dieser Grundlage wurde die Verfügbarkeit der Bilder von Anlagen behutsam ausgeweitet – etwa durch die Aufschaltung von Live-Bildern, jedoch unter Verwendung eines Privacy-Filters – wenn ein zusätzlicher Zweck dies rechtfertigte.

Mehrmals stellte sich die Frage, wie mit einem »technologischen Überschuss« einer Anlage umzugehen sei. Hier geht es um Fälle, in denen das evaluierte Kameramodell technisch raffinierter ist, also etwa über mehr Bild-

[2] Videoordnung der Stadt Winterthur vom 1. September 2013; online abrufbar unter http://stadt.winterthur.ch/treffpunkt-winterthur/und-ausserdem/videoueberwachung/

[3] Die Frist lief gemäss §8 Abs. 2 der Verordnung bis zum 31. Dezember 2013.

[4] Die Videoseite ist zu finden unter: http://stadt.winterthur.ch/treffpunkt-winterthur/und-ausserdem/videoueberwachung/

[5] Mit dem Begriff „Vorfall“ sind Vorkommnisse gemeint, deren Auswertung vom Zweck der Überwachungsanlage gedeckt ist.

auflösung, Zoomreichweite oder Steuerfunktionen verfügt, als dies für den vorgesehenen Überwachungszweck notwendig ist.

Die Datenaufsicht vertrat in solchen Fällen regelmässig die Ansicht, dass solche Probleme in einem ersten Schritt so weit wie möglich technisch oder organisatorisch zu lösen seien – indem beispielsweise die zur Ausübung einer Funktion benötigte Software am Überwachungsarbeitsplatz nicht installiert würde. Schliesslich wurde in solchen Fällen das Reglement mit Massnahmen zur Minderung des Risikos missbräuchlicher Verwendung ergänzt.

Die Datenaufsicht wurde überdies auf kleine Überwachungskameras aufmerksam gemacht, die an bestimmten Kreuzungen der Stadt auf den Lichtampeln montiert waren. Nach einer Besichtigung vor Ort und einer Rückfrage bei der Abteilung Verkehrstechnik der Stadtpolizei konnte der Datenschutzbeauftragte jedoch Entwarnung geben: Bei den Geräten handelte es sich nicht um Kameras, sondern um Lichtsensoren zur Steuerung der Zifferblattbeleuchtung einer an der Ampel festgemachten Uhr.

4. Office 365 an Schulen

Die Datenaufsicht wurde angefragt, ob es möglich wäre, Office 365 an Schulen zu verwenden. Hierbei handelt es sich um eine Online-Version der Office Suite. Das Angebot sollte überdies aus Kostengründen nicht von Microsoft Schweiz, sondern von Microsoft Deutschland bezogen werden.

Das Angebot von Microsoft Deutschland fiel ausser Betracht. Die Verwendung des deutschen Angebots hätte zu einer zu komplexen vertrags- und aufsichtsrechtlichen Situation geführt; die Kontrolle der Schulen über die Daten sowie die Wahrnehmung der entsprechenden Aufsichtsfunktion durch die Datenaufsicht wären kaum durchzusetzen gewesen.

Der Datenschutzbeauftragte prüfte die Geschäftsbedingungen von Microsoft Schweiz in Bezug auf die online Version von Office und kam zum Schluss, dass die vertraglichen Bedingungen nicht den Anforderungen des IDG entsprachen.[6] Aus der Erfahrung heraus war kaum zu erwarten, dass Microsoft sich auf eine Spezialvereinbarung mit der Stadt Winterthur einlassen würde. Entsprechend kam eine Verwendung der Online-Suite vorerst nicht infrage.

Im Laufe des Jahres zeigte sich, dass etliche Schulen in anderen Gemeinden und Kantonen das Online-Angebot nutzen wollten und das Thema verschie-

[6] Insbesondere, was den geografischen Ort der Datenspeicherung sowie die Wahl von Schweizer Recht unter schweizerischer Gerichtsbarkeit betraf.

dene Datenschutzbehörden in der ganzen Schweiz beschäftigte. Ende Jahr konnte Privatim, die Vereinigung der Schweizerischen Datenschutzbeauftragten, zu deren Mitgliedern die Datenaufsicht Winterthur zählt, verkünden, dass Microsoft eingewilligt hatte, die Vertragsbedingungen für Schweizer Bildungsinstitutionen an die Vorgaben des Schweizerischen Datenschutzrechts anzupassen. Durch eine Ergänzung der allgemeinen Geschäftsbedingungen verpflichtete sich Microsoft insbesondere, die Nutzerdaten der Schülerinnen und Schüler nicht für Werbezweck zu verwenden und die Dateien der Nutzer in Europa zu speichern.[7]

Durch Unterschreiben der Zusatzbedingungen können Schulbehörden, die Microsoft Office 365 verwenden möchten, die vertragliche Grundlage mit den Anforderungen des Datenschutzrechts in Einklang bringen.

5. Filtrierung der Google-Suche an Schulen

Von privater Seite wurde die Datenaufsicht angefragt, wie die Filterung des Internetzugangs der Schulen durch Swisscom funktioniere und inwiefern sich dies mit dem Datenschutz und insbesondere auch mit der Datensicherheit vereinbaren lasse. Das Thema hatte die Datenaufsicht zu der Zeit schon eine Weile beschäftigt, zumal auf nationaler Ebene der Datenschutzbeauftragte des Kantons Basel-Stadt bereits auf die Problematik hingewiesen hatte.

Im Rahmen des Programms »Schulen ans Netz« bietet Swisscom eine Filtrierung von Suchergebnissen der Suchmaschine Google an. Dadurch soll verhindert werden, dass Schülerinnen und Schüler bei der Benutzung von Schul-PCs unangemessene Inhalte finden. Seit Oktober 2013 laufen die Suchanfragen mittels SSL über einen verschlüsselten Server. Um die Suchanfragen trotz Verschlüsselung lesen und sortieren zu können, begann die Swisscom, welche die Schulanbindung ans Netz sicherstellt, die Suchanfragen über einen eigenen Server umzuleiten, diese dort zu entschlüsseln und nach erfolgter Filtration erneut zu verschlüsseln und an Google weiterzuleiten.

Diese Umleitung funktioniert nur dann reibungslos, wenn der PC des Nutzers nach wie vor denkt, er wäre mit einem Server von Google verbunden. Da es sich hierbei aber um einen Server der Swisscom handelt, wird dieser mittels eines Zertifikats der US-Amerikanischen Sicherheitsfirma ZScaler als Server von Google ausgegeben. Die hiermit zusammenhängenden Probleme

[7] Weitere Informationen sind abrufbar unter: http://www.privatim.ch/de/privatim-Nachrichten/cloud-computing-im-schulbereich.html

sind nicht von der Hand zu weisen.

Erstens liegt der Sinn einer Verbindung mittels HTTPS gerade darin, dass man sicher sein kann, mit dem richtigen Anbieter verbunden zu sein. Die Zwischenentschlüsselung durch Swisscom mittels Zertifikaten, die (für den jeweiligen Computer) vermeintlich von Google stammen, untergräbt das Vertrauensprinzip, auf dem die SSL-Verschlüsselung mittels Zertifikaten aufbaut; eine Verschlüsselungsarchitektur, die auch von der Stadtverwaltung in sensiblen Bereichen für den Datenaustausch verwendet wird.

Zweitens eröffnet ein Zertifikat, das nur vermeintlich von Google stammt, einen unnötigen Angriffsvektor für allerlei technologischen Schabernack. Ist es erst einmal auf einem PC installiert, akzeptiert dieser die Zertifikate dieser Firma, welche Server falsch identifizieren.

Momentan wird diese Methode nach wie vor verwendet. Nach Ansicht der Datenaufsicht sollte darüber nachgedacht werden, ob die Beeinträchtigung einer weltweit standardisierten Sicherheitsarchitektur, auf welcher der sichere globale Datenverkehr beruht, den vermuteten Gewinn an Jugendschutz aufwiegt.[8] Es wäre möglicherweise sinnvoller, eine weniger riskante Methode der Filtration einzusetzen und möglichen Erleichterungen des Zugangs zu bedenklichem Material pädagogisch zu begegnen.

6. Schulungen und Vorträge

6.1 Schulung der neuen Kaderleute

Im Berichtsjahr hielt der Datenschutzbeauftragte einen Vortrag im Rahmen der Einführungsschulung für neue Kader der Stadtverwaltung. Das Referat wurde im Hinblick auf das Feedback sowie die eigenen Eindrücke der letzten Jahre inhaltlich neu ausgerichtet.

Anstelle einer Einführung zum Datenschutzrecht verschob sich das Augenmerk von Beginn weg auf Fragen aus dem Alltag der städtischen Behörden; der rechtliche Hintergrund wurde auf ein notwendiges Minimum beschränkt. In der Folge erschienen die Teilnehmerinnen und Teilnehmer interessiert und engagiert und – soweit dies in 20 Minuten möglich ist – wurden einzelne Fragen aufgeworfen und diskutiert.

Im Lichte dieser positiven Entwicklung wird die Datenaufsicht die Präsentation und den Inhalt für die kommenden Kurse entlang des eingeschlagenen

[8] »Vermeintlich« deshalb, weil Kinder ausserhalb des Klassenzimmers auf vielfältige Weise nach den verbotenen Begriffen Suchen können.

Weges weiterentwickeln.

7. Laufende Projekte

7.1 Projekt Fokus

Im Berichtsjahr schritt die Planung für das Projekt Fokus weiter. Die Datenaufsicht wurde beigezogen, um jene Fragen, die anlässlich der Besprechungen im Vorjahr ins Visier genommen waren nun im Detail zu besprechen.

Es zeigte sich insbesondere, dass die Konzeption der Arbeitsplätze als Grossraumbüros eine gewisse Herausforderung für den Schutz von Personendaten darstellen wird. Dies sowohl in Bezug auf die bearbeiteten Daten der Winterthurerinnen und Winterthurer als auch in Bezug auf die Privatsphäre der Angestellten sowie deren von Amtes wegen zu wahrenden Geheimnisse.[9]

Das Aufteilungskonzept der Stockwerke sieht vor, dass Ämter grundsätzlich zusammenbleiben, dass jedoch auf gewissen Stockwerken sogenannte Begegnungszonen eingerichtet werden. Hier war nach Ansicht des Datenschutzbeauftragten darauf zu achten, dass Bereiche mit unterschiedlichem Risikoprofil in Bezug auf den Datenschutz keine frei zugängliche Begegnungszone teilten. Entsprechend wurden die Zonen so gelegt, dass sensible Bereiche von den Begegnungszonen aus nicht frei zugänglich, sondern nur mit vorheriger Identifikation zu erreichen sind.[10]

Weiter sind Sitzungszimmer geplant, die im Gegensatz zu „internen“ Sitzungszimmern auch von „externen“[11] Personen genutzt werden können.

Hier wies die Datenaufsicht darauf hin, dass externe Sitzungszimmer, die nur mittels Durchquerung des offenen Bürobereichs einer Abteilung zu erreichen sind, ein unnötiges Risiko darstellten, da externe Benutzer des Sitzungszimmers notwendigerweise an Arbeitsplätzen vorbeigehen müssten. Es bestehe daher ein erhöhtes Risiko, dass externe Sitzungsteilnehmer auf dem Weg zum Sitzungszimmer Personendaten wahrnehmen könnten. Je nach Abteilung könne es sich zudem um besonders schützenswerte Personendaten handeln oder gar um solche, die den strafrechtlichen Bestimmungen in Bezug auf Amts- und Berufsgeheimnisse unterstehen.

Zur Senkung dieses Risikos wurden die Standorte für externe Sitzungszim-

[9] Hierunter fallen beispielsweise medizinische Daten, etwa aus den Bereichen Personal, Schulen, soziale Dienste.

[10] Hierunter fallen Zutrittskontrollen mittels Badge oder Sonnerie.

[11] Personen von ausserhalb der betreffenden Verwaltungseinheit sowie auch Mitglieder von parlamentarischen Kommissionen.

mer neu evaluiert und jeweils in den Eingangsbereich eines offenen Bürobereichs verlegt, gleich neben der Liftanlage und den Treppen.

Schliesslich verständigte sich die Datenaufsicht mit der Projektleitung darauf, dass der Datenschutzbeauftragte in die Projektgruppe Sicherheit eingeladen wird, um die Entwicklung der Sicherheitsmassnahmen beratend zu begleiten. Hier wird insbesondere die Ausarbeitung einer handhabbaren „Clean-Desk Policy“ für die Grossraumbüros des Superblocks im Vordergrund stehen.

7.2 Datenbank GREKOS

Das Projekt GEKOS (Grundsteuern, Einwohnerkontrolle, ordentliche Steuern) soll die bestehenden Informatiklösungen in den Bereichen, Steuern, Einwohnerkontrolle und Feuerpolizei ablösen und integrieren. Hierbei entsteht eine Datenbank, die den genannten Bereichen zur Verfügung steht und zugleich als technische Grundlage für die Gewährung von Zugriffsrechten anderer Stellen dient. Dies betrifft insbesondere das Einwohnerregister der Einwohnerkontrolle, die aufgrund § 38 Abs. 2 des Gemeindegesetzes befugt ist, anderen Stellen Zugriff zu gewähren, sofern deren Bearbeitung im Einklang mit den Vorschriften des IDG steht.

Im Rahmen der Evaluation der Software wurde die Datenaufsicht erstmals eingeladen, eine Stellungnahme abzugeben. Diese Gelegenheit nahm der Datenschutzbeauftragte zum Anlass, vorgängig mit den Projektverantwortlichen das Gespräch zu suchen und darauf hinzuweisen, dass die Software insbesondere eine möglichst feingliedrige Zuteilung von Rechten und Pflichten auf einzelne Personen ermöglichen müsse.

In der nun vorliegenden Lösung wird diese Vorgabe erfüllt, indem zwei technologisch unterschiedliche Zugriffsvarianten zur Anwendung gelangen. Einerseits wird die Einwohnerkontrolle im Rahmen der Software NEST über einen vollen Zugriff auf sämtliche Daten verfügen. Daneben können externe Stellen einen Zugriff über ein spezielles Web-Interface erhalten, das eine vollständig flexible Zuteilung der Zugriffsrechte pro Datensatz erlaubt.

Derzeit ist die Datenaufsicht nun daran, die Einwohnerkontrolle bei der Überprüfung der eingegangenen Zugriffsanfragen zu unterstützen. Die Evaluation sämtlicher Anfragen wird voraussichtlich bis Mitte 2014 andauern.

8. Internes

8.1 Zwischenrevision der Finanzkontrolle

Die Datenaufsichtsstelle wurde im Berichtsjahr einer Zwischenrevision der Finanzkontrolle unterzogen. Geprüft wurde die Buchhaltung der zugehörigen Kostenstelle sowie die Organisation und interne Kontrolle der Finanzprozesse. Grundlage hierfür war ein Gespräch zwischen dem Datenschutzbeauftragten und der Vertretung der Finanzkontrolle, sowie die Buchungsbelege der Datenaufsicht für die Periode vom 1. Januar 2012 bis zum 22. Juli 2013.

Die Finanzkontrolle gelangte zum Ergebnis, dass die Buchhaltung der Aufsichtsstelle gut geführt und zweckmässig organisiert sei.

9. Ausblick

In den folgenden Jahren werden sich nach meiner Ansicht einige Entwicklungen beschleunigen, welche die Risiken für die Privatsphäre und die informationelle Autonomie der Einwohnerinnen und Einwohner Winterthurs sowie auch der städtischen Angestellten erhöhen.

Zu nennen sind hier etwa die Zentralisierung von Datenbeständen der Stadtbehörden, die Auslagerung elektronischer Datenbearbeitungen an externe Hostinganbieter, die technologische Beaufsichtigung von Mitarbeiterinnen und Mitarbeitern der Stadtverwaltung, die statistische Durchdringung des städtischen Gefüges und seiner Bewohnerinnen und Bewohner Zwecks politischer Planung, sowie das E-Government, also die Bereitstellung von Dienstleistungen der Stadtverwaltung über das Internet. Wenig überraschend wäre auch, wenn das Thema der Videoüberwachung sich allenthalben wieder in den Vordergrund drängte.

Kennzeichen dieser Entwicklung ist, dass die Betroffenen dieser Datenbearbeitungen eine zunehmend unklare Vorstellung davon haben werden, welche Daten über sie bearbeitet werden, geschweige denn, in welchen Zusammenhängen diese Bearbeitung geschieht; längerfristig droht die Entstehung einer virtuellen Parallelidentität, die eine Eigendynamik entwickeln kann und für die Betroffenen inhaltlich und geografisch unüberschaubar wird. Dadurch drohen die Informationsrechte, welche die Datenschutzgesetze den Rechtssubjekten zugestehen, ins Leere zu laufen.

Aufgabe der Datenaufsicht wird es sein, die zunehmend verminderte Wirk-

samkeit der datenschutzrechtlichen Einsichtsrechte durch Begleitung und Beaufsichtigung der städtischen Behörden so gut wie möglich auszugleichen.

Für die städtischen Behörden wiederum birgt diese Entwicklung gewisse subtile Risiken. Durch die Auslagerung von Datenbearbeitungen geben sie die Kontrolle über Sicherheit und Verfügbarkeit der Daten an private Anbieter ab. Denn für die in den entsprechenden Verträgen vorgesehenen Audits fehlen die Ressourcen - sowohl bei den Behörden selbst wie auch bei der zuständigen Aufsichtsstelle.

Winterthur, 26. Mai 2014 Datenaufsichtsstelle Stadt Winterthur

Philip Glass, Datenschutzbeauftragter

10. Anhang

10.1 Thematische Übersicht

Im Berichtsjahr bearbeitete der Datenschutzbeauftragte Anfragen von Behörden und Privatpersonen in den folgenden Bereichen.

- Cloudspeicher, Voraussetzungen der Nutzung, Evaluation einer städtischen Lösung
- Denkmalschutz, Publikation schutzwürdiger Bauten
- Einwohnerkontrolle, Steueramt, Softwaremigration, Zugriffsmatrixen zentralisierter Datenbanken, Zugriff durch andere städtische Behörden
- Fernsehinterview zum Thema Datenschutz
- Flottenoptimierung mittels GPS
- Forschung, Verwendung von städtischen Daten
- Glasfasernetze, Verlegung und Vermarktung, Wohnungsdaten, Kontaktdaten, vertragliche Einbindung von Dritten
- Grossraumbüros, Informationsmanagement und Geheimhaltungspflichten, Besucherstromführung, technische Sicherungssysteme
- Informationssicherheit und Datenschutz, Risikomanagement bei städtischen Projekten, Bedarfsprüfung durch Formular der IDW
- Informationssicherheit, Mitarbeiterüberwachung am Arbeitsplatz
- Kontrolltätigkeit, Vorgehen, Fragekataloge, Beizug externer Auditoren
- Landeskirche, Datenschutzrevers
- Löschungsanspruch bezüglich Beschlüsse der städtischen Organe im Internet, Durchsetzung der Rechte aus dem IDG, Einrichtung Prozessablauf
- Mobile Device Management, Bring your own device, Geräteortung, Verwendung von iPads durch die Polizei

- Öffentlichkeitsprinzip, Akteneinsicht in Beratungsprotokolle, Polizeiprotokolle
- Office 365, Software Suite »Lehreroffice«
- Outsourcing, Durchsetzung AGB des Kantons Zürich, Beurteilung von Zertifikaten, Anwendung in Mehrparteienverhältnissen
- Personalrecht, elektronische Personaldossier, Bewerbungen, Umgang mit Absenzen, Betreuung durch Personalärzte, medizinischer Datenaustausch
- Persönlichkeitsschutz im Rahmen von Dokumentarfilmen
- Revision der Buchhaltung, Budgetierung
- Schulnetze, Datensicherheit, Sinn von Passwörtern, Sensibilisierung von Schülerinnen und Schülern, Filterung von Suchergebnissen
- Sicherheitsanforderungen an Statistikserver
- Statistiken in den Bereichen Stromverbrauch, Wirtschafts- und Stadtentwicklung,
- SuisseID
- Vereinheitlichung der Spitexrichtlinie des Kantons Zürich
- Verwendung von sozialen Netzwerken in Schulen und Verwaltung
- Videoordnung, Ausarbeitung, Umsetzung
- Videoüberwachung der Stadtpolizei, Anwendung der neuen kantonalen Bestimmungen
- Videoüberwachung, Beratung und Prüfung von Reglementen
- Vorgehen bei offensichtlichen Missbräuchen der IT-Infrastruktur, Auslegung des Nutzungsreglements

10.2 Bearbeitungsstand der Dossiers per 31. Dezember 2013

Jahr	Eingänge	Erledigungen	Pendent
2011	75	59	16
2012	59	54	21
2013	80	65	36

10.3 Aufschlüsselung der Neueingänge nach Aufgaben gemäss § 34 IDG

Aufgabe	Anzahl Dossiers
Beratung der städtischen Behörden	35
Beratung von Privaten	13
Überwachung der Durchführung des Datenschutzrechts	
- anlassgebundene Kontrollen	5
- anlassfreie Kontrollen	-
Vorabkontrollen	3
Vermittlung zwischen Behörden und Privaten	-
Information der Öffentlichkeit über den Datenschutz	1
Beurteilung von Erlassen und Reglementen	7
Stellungnahmen an Behörden	3
Angebot Aus- und Weiterbildung in Fragen des Datenschutzes	
- Angebot der Datenaufsicht	1
- Auf Anfrage einer Behörde	1
Zusammenarbeit mit anderen Datenschutzbehörden	2
Interne Aufgaben (Organisation, Buchhaltung, Jahresbericht)	9