Stadt Winterthur

Tätigkeitsbericht 2014

des Datenschutzbeauftragten der Stadt Winterthur

an den Grossen Gemeinderat der Stadt Winterthur

Berichtsperiode vom 1. Januar 2014 bis zum 31. Dezember 2014

Inhaltsverzeichnis

§ 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. Das Berichtsjahr in Kürze

Nachdem der Erlass der städtischen „Videoordnung“ im Jahr davor für einen aussergewöhnlichen Anstieg der Fallzahlen geführt hatte, liegt die Zahl der Neueingänge im Berichtsjahr etwas tiefer, im Mittelfeld der vergangenen vier Jahre. Dies führte dazu, dass der Anstieg der Pendenzen weniger stark ausfiel als im Vorjahr. Dennoch bewegen sich diese in einem Bereich, der sich stetig der durchschnittlichen jährlichen Erledigungszahl annähert. Eine Übersicht über die Fallzahlen der letzten Jahre ist im Anhang des Berichts zu finden.

Thematisch war das Berichtsjahr sehr variiert. Einen gewissen Schwerpunkt bildete die Prüfung der Zugriffsberechtigungen auf die neue Datenbank NEST der Einwohnerkontrolle. Weiter begleitete die Datenaufsicht die Projektgruppe FOKUS, welche den sehr aufwendigen und komplexen Umzug in den neuen Superblock organisiert. Ein wichtiger Punkt in diesem Zusammenhang ist die Erarbeitung einer Richtlinie über den Vertraulichen Umgang mit Information in den neuen Grossraumbüros. Diese ist weit gediehen und sollte zum Zeitpunkt des Umzugs in der Endfassung als Merkblatt verfügbar sein. Im Abschnitt „Laufende Projekte“ ist der gegenwärtige Stand der Dinge kurz dargestellt.

Anfragen seitens privater Personen sind im Berichtsjahr leicht zurückgegangen, was im Hinblick auf die ohnehin kleinen Fallzahlen in diesem Bereich vor allem bedeutet, dass sie nicht zugenommen haben. Mit Blick auf die aktuellen Ressourcen der Datenaufsicht wird sich daran in den nächsten Jahren wohl wenig ändern.

Schliesslich hat die Datenaufsicht im Berichtsjahr keine fachlichen Schulungen durchgeführt und keine Aufträge für externe Audits vergeben. Entsprechende Projekte sind in Planung, erweisen sich jedoch regelmässig als sehr aufwendig und zeitintensiv.

2. Ausgewählte Fälle

2.1 Prüfung der Zugriffsmatrix NEST

Die Datenaufsicht berichtete bereits im letzten Jahresbericht von den laufenden Zuteilungen der Zugriffsrechte auf die Datenbank der Einwohnerkontrolle, einem Teilbereich des Projektes GREKOS.[1] Diese Arbeiten konnten mittlerweile vorerst abgeschlossen werden. Hierbei zeigte sich, dass das Erfordernis, die gewünschten Zugriffsrechte zu begründen, die städtischen Behörden dazu brachte, ihre jeweiligen Datenbedürfnisse zu prüfen und anzupassen. Unter dem Strich wurde die Berechtigungsliste im Vergleich zu den Vorgängersystemen merklich schlanker. So wurde in

[1] Informationen zu GREKOS sind online abrufbar: http://informatikdienste.winterthur.ch/projekte/grekos/

vielen Fällen schliesslich auf den Zugriff auf Kategorien wie Konfession, Beziehungen, Wohngemeinschaft, Nationalität, Geburtsort, Arbeitgeber, Sorgerecht oder vormundschaftliche Massnahmen verzichtet.

Als eine der Knacknüsse erwies sich die neue Versicherungsnummer der AHV, bekannt unter dem Kürzel „AHVN13“. Die Verwendung der Versicherungsnummer wird durch das AHV-Recht des Bundes geregelt und darf nur unter Beachtung strikter gesetzlicher Voraussetzungen systematisch erfolgen. Mit systematisch ist unter anderem auch gemeint, dass die Nummer ohne Gegenprüfung der bekannt gebenden Stelle durch ein automatisches Abrufverfahren in eine eigene Datenbank eingelesen werden kann, um Datensätze zu identifizieren. Folglich durfte der Zugriff auf die in der Datenbank der Einwohnerkontrolle gespeicherte AHVN13 nur unter Nachweis einer ausdrücklichen gesetzlichen Grundlage freigeschaltet werden.

In einigen Fällen konnte dieser Nachweis erbracht werden. Andere Stellen, welche die Nummer beispielsweise als Identifikator zum Abgleich mit einer kantonalen Datenbank nutzen wollten, hierfür aber keine genügende gesetzliche Grundlage angeben konnten, mussten alternative Methoden prüfen. Als brauchbarer Ersatz erwiese sich in diesen Fällen oft die alte AHV-Nummer, die noch parallel zur AHVN13 geführt wird.

2.2 Vorabkontrolle: Pilotbetrieb Personalärztliches Konzept A & P

Die Stadt Winterthur ist als Arbeitgeberin in gewissen Bereichen gesetzlich verpflichtet, Massnahme zum Schutz von Mitarbeiterinnen und Mitarbeitern sowie von Klientinnen und Klienten zu treffen. Aus diesem Grund wurde für den Bereich Alter und Pflege ein Pilotprojekt für den Betrieb eines personalärztlichen Dienstes erarbeitet und der Datenaufsicht zur Vorabkontrolle gemäss § 10 IDG vorgelegt.

Das Konzept sah vor, dass die medizinische Poliklinik des Kantonsspitals Winterthur personalärztliche Aufgaben für die Mitarbeitenden des Bereichs Alter und Pflege übernimmt. Hierzu zählen Massnahmen zur Verhütung von Betriebsunfällen und Berufskrankheiten. Die Aufzählung der Massnahmen orientierte sich in weiten Teilen an der einschlägigen Gesetzgebung des Bundes[2] sowie an der kantonalen Richtlinie Gesundheitsschutz, welche die Kontrolle des Gesundheitszustandes von Lernenden der Berufe „Fachfrau/Fachmann Gesundheit EFZ“ und "Assistent/-in Gesundheit und Soziales EBA" betrifft.

Der Aufgabenkatalog sah vor, dass der personalärztliche Dienst eine Gesundheitsakte führt, die Abklärungen der gesundheitlichen Voraussetzungen für die Berufsausübung von definierten Funktionsgruppen vornimmt, insbesondere die Gesund-

[2] Bundesgesetz über die Unfallversicherung (UVG, SR 832.20), VO über die Unfallversicherung (UVV, SR 832.202), VO über die Verhütung von Unfällen und Berufskrankheiten (VUV, SR 832.30), Arbeitsgesetz (ArG, SR 822.11), EKAS-Richtlinie Nr. 6508 über den Beizug von Arbeitsärzten und anderen Spezialisten der Arbeitssicherheit (abrufbar unter http://www.ekas.admin.ch/).

heitsabklärung zu Beginn und Ende der Ausbildung sowie die Abklärung der Tauglichkeit für Nachtarbeit. Weiter sind prophylaktische Massnahmen zum Schutz vor Infektionskrankheiten vorgesehen, namentlich ein Eintrittsgespräch bei neuen Mitarbeitenden sowie die Durchführung gewisser gesetzlich vorgeschriebener Impfungen.

Das Konzept regelt auch die Schweigepflicht sowie die Einsicht in die Gesundheitsakte, die nur der zuständigen Ärztin bzw. dem zuständigen Arzt und der betroffenen Person zusteht. Zudem war vorgesehen, dass mögliche vertrauensärztliche Abklärungen jeweils von einer anderen Medizinfachperson durchgeführt werden müssten.

Die Datenaufsicht klärte mit den zuständigen Personen einige Details des Konzepts und regte insbesondere an, dass die personelle Trennung von personal- und vertrauensärztlichen Dienstleistungen sich in der Führung getrennter Dossiers für die beiden Funktionen spiegle. Zudem sei die Vorschrift sorgfältiger zu formulieren, wonach bei Eintrittsgesprächen Personen mit Migrationshintergrund besonders zu beachten seien. Hier sei nicht die Herkunft, sondern der möglicherweise damit zusammenhängende Aufenthalt in Risikogebieten ausschlaggebend. Zudem sollten einige der Grundlagen präziser formuliert werden, und dabei vor allem die zulässigen Massnahmen und korrespondierenden gesetzlichen Grundlagen genauer bezeichnet werden.

In der Folge wurde das Konzept angepasst, was dazu führte, dass die Datenaufsicht anlässlich der Vernehmlassung auf eine detaillierte Stellungnahme verzichten konnte.

2.3 Eskalation von Zugriffsrechten über MS Word

Die Datenaufsicht wurde auf eine Lücke in der Berechtigungsverwaltung der stadtweit verwendeten elektronischen Geschäftskontrolle iGEKO aufmerksam gemacht. Über die Funktion [Datei öffnen] => [Zuletzt besuchte Orte] war es möglich, ohne die nötigen Zugriffsrechte der Geschäftskontrolle temporäre Dokumente in Word zu öffnen.

Auf Meldung der Datenaufsicht hin eröffnete der Datensicherheitsbeauftragte der IDW einen Informationssicherheitsvorfall. Hierbei handelt es sich um einen vordefinierten Prozessablauf, nach dem in Fällen von festgestellten Verletzungen oder Gefährdungen der Datensicherheit vorgegangen wird.

Die nachfolgende Untersuchung führte zur Erkenntnis, dass aufgrund eines Fehlers im Berechtigungssystem der Geschäftskontrolle ein Zugriff auf Dokumente möglich war, die bereits für andere Nutzer freigegeben worden und aus technischen Gründen während 24 Stunden in einem temporären Ordner auf einem Netzlaufwerk gespeichert wurden. Als Sofortmassnahme wurde diese Zwischenspeicherung auf 10

Minuten reduziert.

Da die betroffenen Dokumente auf der Ebene der Zwischenspeicherung durch die Applikation iGEKO nicht mit Klarnamen, sondern einem Nummerncode als Bezeichnung gespeichert werden, wäre die Suche nach einem bestimmten Dokument sehr aufwendig gewesen, was das Risiko einer gezielten Ausforschung in Grenzen hielt. Durch die Verringerung der Speicherzeit wurde auch das Risiko eines Zufallsfundes durch Nutzer von Computern des Stadtnetzes auf ein kurzfristig vertretbares Mass reduziert.

Zwei Wochen später konnte die Systemkonfiguration der elektronischen Geschäftskontrolle geändert und die Lücke damit geschlossen werden.

3. Einsitz in der Arbeitsgruppe IDG

Im März 2014 war der Datenschutzbeauftragte eingeladen, an der 8. Sitzung der AG IDG teilzunehmen. Zweck der AG ist die Anpassung der städtischen Gesetzgebung an die Vorgaben des kantonalen Informations- und Datenschutzgesetzes. Zur Diskussion stand der Regelungsbedarf im Bereich der Bearbeitung von Personendaten nach dem Erlass der Verordnung über die Bearbeitung besonderer Personendaten vom 16. September 2013.

In Bezug auf einfache Personendaten sah der Datenschutzbeauftragte kein Handlungsbedarf, da in diesen Fällen die Erlaubnis zur Bearbeitung sich aus der Rechtsgrundlage der zugrunde liegenden Aufgabe ergibt.

In Bezug auf besondere Personendaten stellte die AG insbesondere in den Bereichen Pflege und Sozialhilfe gewisse Unklarheiten in den gesetzlichen Grundlagen fest, die jedoch auf kantonaler Ebene zu regeln seien. Diese Meinung teilte der Datenschutzbeauftragte insofern, als sich erst in der Anwendung der teilweise relativ „jungen“[3] kantonalen Vorschriften zeigen würde, ob weiterer Handlungsbedarf bestehe. Sollten sich im Laufe der Zeit Anpassungen aufdrängen, wäre auf den Entscheid zurückzukommen.

Als weiterer Punkt wurde die Überführung der Richtlinie „Sofortmassnahmen zur Einführung des Öffentlichkeitsprinzips“ des Stadtrates vom 1. Oktober 2008 in eine Verordnung des Stadtrates diskutiert. Ergänzend zur bisherigen Richtlinie soll diese Verordnung die Geheimhaltung der Mitberichte im Stadtrat sowie die dezentralisierte Auskunft bei Informationszugangsgesuchen regeln. Nachdem auf dem Zirkularweg Vorschläge eingebracht wurden, ist ein erster Entwurf in Bearbeitung.

[3] Die letzte Änderung des kantonalen Gesetzes über die Sozialhilfe ist seit dem 1. Januar 2013 in Kraft.

4. Schulungen und Vorträge

4.1 Schulung der neuen Kaderleute

Die Datenaufsicht erhielt im Berichtsjahr erneut die Gelegenheit, neuen der Stadtverwaltung die Vorgaben und Anliegen des Datenschutzes zu vermitteln. Wie im Vorjahr bestand das Ziel vorwiegend darin, die Datenaufsicht als Anlaufstelle für datenschutzrechtliche Fragen bekannter zu machen.

Aufgrund der sehr knappen Zeit von einer Viertelstunde konnte das Thema selbst jedoch nur sehr oberflächlich behandelt werden. Der Sinn der Veranstaltung liegt denn auch mehr in der Vorstellung der verschiedenen zentralen Bereiche der Stadtverwaltung sowie der unabhängigen Aufsichtsbehörden und der Stadtkanzlei als in einer fachlichen Schulung.

4.2 Projektwoche Datenschutz und Kryptografie KS Im Lee

Die Kantonsschule Im Lee fragte an, ob es möglich wäre, im Rahmen der Projektwoche „Datenschutz und Kryptografie“ eine lose Fragestunde mit dem Datenschutzbeauftragten durchzuführen. Nach einer kurzen Besprechung in Bezug auf Zweck und Inhalt dieser Fragerunde, lud der Datenschutzbeauftragte die Schülerinnen und Schüler mit den betreuenden Lehrpersonen in den grossen Saal des alten Stadthauses. Das Timing erwies sich als perfekt, da der Saal aufgrund einer Musikveranstaltung am Abend mit voller Konzertbestuhlung aufwartete.

Der Datenschutzbeauftragte erzählte zu Beginn etwas über die Aufsichtsstelle, die Funktionen des DSB sowie einige aktuelle Themen. Die Schülerinnen und Schüler ihrerseits wirkten motiviert mit und stellten Fragen über viele Bereiche des digitalen Alltags, zu sozialen Netzwerken, Videokameras, E-Mail-Sicherheit und vielem mehr.

Aus Sicht der Datenaufsicht war die Veranstaltung ein Erfolg, insbesondere da auch die anwesenden Lehrpersonen das informelle Format schätzten und meinten, die Schülerinnen und Schüler hätten sehr aktiv mitgewirkt.

5. Laufende Projekte

5.1 Merkblatt „Vertraulichkeit im Superblock“

Der Datenschutzbeauftragte wurde gebeten, ein Merkblatt über den vertraulichen Umgang mit Daten in den Grossraumbüros des Superblocks herauszugeben.

Mittlerweile hat eine Arbeitsgruppe – zusammengesetzt aus einer Vertreterin der Projektgruppe Fokus, einem Vertreter der Personalentwicklung, einem Vertreter der Personalleitung DFI und dem Datenschutzbeauftragten – sich gebildet, einen Entwurf verabschiedet, und sich wieder aufgelöst.

Hierbei wurde grosser Wert darauf gelegt, eine Lösung zu finden, die einerseits die besonderen Risiken der offenen Bauweise der Grossraumbüros Rechnung trägt, zugleich aber die Mitarbeiterinnen und Mitarbeiter nicht überfordert. Im Zentrum der Diskussion standen die Möglichkeiten und Grenzen von Clean-Desk-Vorgaben, die Handhabung der verschiedenen Zutrittskontrollen für Mitarbeitende und Besucher, die Nutzung zentraler Druckersysteme sowie die Nutzung von Telefonen und Besprechungsräumen.

Die Datenaufsicht legte den Entwurf dem Datensicherheitsbeauftragten der IDW zur Stellungnahme und Ergänzung vor. Zurzeit befindet sich das Merkblatt in einer informellen Vernehmlassung zur Abgleichung der Vorgaben des Entwurfs mit den künftigen tatsächlichen Gegebenheiten im „Superblock"-Gebäude; es wäre sinnlos, Verhaltensanweisungen zu geben, die aufgrund der vorhandenen Infrastruktur nicht eingehalten werden können.

5.2 Ausnahmeregelungen für den Content Filter „Cloud Speicher"

Mit Beschluss vom 21. August 2013 hatte der Stadtrat die Einführung eines Content Filters für das städtische Datennetz beschlossen. Dieser erlaubt die Sperre oder Freischaltung bestimmter Internetadressen für die am Stadtnetz angeschlossenen Computer. Adressen, die auf dieser Liste aufgeführt sind, können auf einer „weissen Liste" eingetragen und so von der Sperrung ausgenommen werden. Der Beschluss des Stadtrates sieht in besonderen Fällen die Möglichkeit vor, auf Gesuch hin einzelne Kategorien für bestimmte Mitarbeiterinnen und Mitarbeiter freizuschalten. Hingegen ist es mit der bestehenden Lösung nicht möglich, einzelne Adressen für einzelne User freizuschalten.

In der Folge gelangten einige Bereiche der Stadt an die IDW mit der Bitte, gewisse Online-Speicherdienste für einige ihrer Mitarbeiterinnen und Mitarbeiter freizuschalten. Als Begründung gaben diese Stellen jeweils an, sie benötigten einen bestimmten Dienst, weil dieser für den Wissensaustausch mit anderen Behörden oder Projekt-Partnern notwendig sei. Zudem läge es nicht in ihrer Hand, welcher Dienst hierfür jeweils verwendet werde.

Die KESB etwa machte geltend, dass sie Zugriff auf einen bestimmten amerikanischen Cloud-Dienst benötige, da die KESB im Kanton über diese Plattform Formulare, Merkblätter und dergleichen austauschten.

Einige kulturelle Institutionen der Stadt machten ebenfalls geltend, auf die Verwendung bestimmter Cloud-Dienste angewiesen zu sein, um im Rahmen von Projekten und Ausstellungen mit Museen im In- und Ausland Informationen auszutauschen.

Die IDW baten die Datenaufsicht um eine Klärung der Rechtslage. Diese gelangte zum Schluss, dass die rechtlichen Vorgaben des IDG aus verschiedenen Gründen je-

weils nicht erfüllt seien,[4] weshalb eine Speicherung von Personendaten auf Servern dieser Dienste nicht zulässig wäre. Aufgrund der Schwierigkeit, die korrekte Nutzung der freigeschalteten Dienste zu kontrollieren, stellt dies auch dann ein rechtliches Problem dar, wenn die geplante Nutzung eines solchen Dienstes durch eine Behörde nur Dokumente ohne Personendaten umfasst.

Als Kompromiss akzeptierte die Datenaufsicht schliesslich die Freischaltung, wenn eine Behörde in dem Bereich, für den die Freischaltung gewünscht war, keine oder nur wenige und/oder unbedenkliche Personendaten bearbeitete oder wenn sie im Vorfeld der Freischaltung griffige Massnahmen zur Verhinderung von Missbrauch einführte und dies anlässlich Gesuchsstellung auch nachweisen konnte.

Zurzeit sind einige Gesuche um Freischaltung hängig, noch ist unklar, welche Massnahmen einen wirksamen Schutz gegen die Verwendung dieser Dienste zur Zwischenspeicherung von Personendaten oder Anlage von Schattendossiers bieten.

6. Internes

6.1 Zusammenarbeit mit anderen Datenschutzbehörden / Weiterbildung

Im Berichtsjahr nahm der Datenschutzbeauftragte an zwei Plenumsveranstaltungen von Privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, teil. Im Vordergrund standen hierbei der Meinungsaustausch mit Datenschutzbeauftragten aus anderen Kantonen und Gemeinden sowie die Planung der künftigen Zusammenarbeit im Rahmen der Vereinigung. Die beiden Veranstaltungen wurden jeweils von öffentlichen Tagungen zum Thema Datenschutz begleitet.

Die erste Veranstaltung fand in Zusammenarbeit mit der zhaw – School of Management and Law im März 2014 statt und befasste sich mit dem Thema der Effizienz und der Wirksamkeit von Kontrollen durch Datenschutzbehörden. Der Datenschutzbeauftragte nahm vor allem mit, dass Kontrollen in der Regel mehrere Tage in Anspruch nehmen und einen langen Vorlauf benötigen.

Die zweite Veranstaltung von Privatim wurde im Oktober 2014 zum Thema „Datenschutzrecht im Gesundheitswesen“ durchgeführt. Von besonderem Interesse war ein Werkstattgespräch zum Thema Datenschutz und IT-Security, das aktuelle Themen und Erfahrungen in diesem Bereich anhand des Beispiels des Zuger Kantonsspitals vermittelte.

Im Dezember 2014 weilte der Datenschutzbeauftragte an einer Tagung der Universität St. Gallen zu diversen aktuellen Themen des Datenschutzrechts. Die Themenpalette reichte von grundsätzlichen Fragen zur Rechtmässigkeit von Datenbearbei-

[4] Einige Dienste speicherten etwa die Daten in den USA, deren Datenschutzniveau nicht jenem vom IDG entspricht, oder räumten sich in ihren AGB das Recht ein, die vertraglichen Grundlagen des Dienstes jederzeit einseitig zu ändern und sahen keine Audit-Rechte der User vor, was wiederum den Befugnissen der Datenschutzbehörden gemäss IDG widersprach.

tungen, über Fragen des Datenschutzrechts im Sozialversicherungsrecht, der Entwicklung im europäischen Datenschutzrecht, der rechtlichen Erfassung allgegenwärtiger Aufzeichnungsgeräte wie etwa Crashrecorder und Dashcams sowie Fragen des Datenschutzes in Gerichtsverfahren im Hinblick auf verschiedene moderne Methoden der Beweismittelerhebung. Das letztgenannte Thema ist durchaus auch für staatliche Behörden von gemeinhin unterschätzter Brisanz, die zunimmt, je mehr Daten die Stadtverwaltung aufzeichnet und speichert.

7. Ausblick

Am 3. Dezember 2014 wurde der Datenschutzbeauftragte für eine zweite Amtsperiode bis Ende 2018 gewählt. Da im Vergleich zum Amtsantritt im Januar 2011 die Eingewöhnungszeit wegfiel, konnte sogleich mit einer langfristigen Planung begonnen werden.

Das hauptsächliche Augenmerk für die nächsten Jahre liegt dabei auf jenen Aufgaben in § 34 IDG, die der Datenschutzbeauftragte bisher nicht wahrnehmen konnte, namentlich Kontrollen, Datenaudits, Weiterbildungsangebote für städtische Rechtsdienste sowie Veranstaltungen zum Thema Datenschutz und Datensicherheit an Schulen.

Es ist hierbei nicht ausgeschlossen, dass die Datenaufsicht im nächsten Jahr die Beratung der städtischen Behörden für eine gewisse Zeit zugunsten dieser Projekte aussetzen wird. Nach vier Jahren Beratung ist es an der Zeit, die Umsetzung zu überprüfen.

Winterthur, 12. Mai 2015 Datenaufsichtsstelle der Stadt Winterthur

Philip Glass, Datenschutzbeauftragter

8 Anhang

8.1 Thematische Übersicht

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

- → Budget, Betrieb der Aufsichtsstelle, Optimierung der Zusammenarbeit mit Ratsleitung und Dienststellen der Stadt
- → Content Filter, Sperrung von Cloud-Diensten, Auskunft über Negativlisten
- → Datenbekanntgabe, Adressen von Neugeborenen an Pro Juventute
- → Datensicherheit, Zugriffsrechte, Abwesenheitsprozeduren, Rechenzentren der IDW, Schulnetze
- → Forstbetriebe, Webauftritt, Online Shop
- → Geodaten, Nutzungsberechtigung
- → GREKOS, Verbunddatenbanken, Prüfung der Architektur, Bereichslösung NEST der Einwohnerkontrolle, Zugriffe städtischer Behörden, Zugriffe von Privaten mit öffentlichem Auftrag
- → Grossraumbüros, Vertraulichkeit, Zutrittskontrollen
- → Öffentlichkeitsprinzip, Beschlussprotokolle, Gebühren Albanifest, Sperrlisten Content Filter
- → Outsourcing von Servern und Applikationen
- → Personalführung, Durchführung der Personalbefragung, Anonymität der Teilnehmenden, Auskunft über Ergebnisse, Personalärztliches Konzept Alter & Pflege, elektronisches Bewerbungsmanagement, elektronisches Personaldossier
- → Polizeirapporte, POLIS-System der Stadtpolizei, Speicherung von Daten, Informationsauskunft an Private
- → Privacy-Zertifikate
- → Schulinformatik, Überwachung von PCs, Nutzung von Office und Cloud-Diensten, Schulnetze
- → Smartmetering, automatische Auslesung, statistische Nutzung
- → Softwareverträge, Anpassung von AGB, AGB SIK
- → Statistik, Nutzung städtischer Daten, Anonymität, Untersuchung bestimmbarer Personengruppen, Datenlieferung an die SKOS
- → Überwachung, Umsetzung der Videoordnung, Private Überwachung, Auswertung von Systemstartzeiten zur Präsenzkontrolle
- → Webcams, Auflösung, Schwenkbereich, Verpixelung einsehbarer Fenster und Balkone, Einsichts- und Änderungsrechte

8.2 Bearbeitungsstand der Dossiers per 31. Dezember 2014

Jahr	Eingänge	Erledigungen	Pendent	Jahrestotal
2011	75	59	16	75
2012	59	54	21	75
2013	80	65	36	101
2014	68	58	46	104

8.3 Aufschlüsselung der neuen Dossiers nach Aufgaben gemäss § 34 IDG

Aufgabe	Anzahl Dossiers
Beratung der städtischen Behörden	37
Beratung von Privaten	10
Überwachung der Durchführung des Datenschutzrechts	
- anlassgebundene Kontrollen	-
- anlassfreie Kontrollen	-
- Vorabkontrollen	3
Vermittlung zwischen Behörden und Privaten	-
Information der Öffentlichkeit über den Datenschutz	-
Beurteilung von Erlassen und Reglementen	3
Stellungnahmen und Berichte	3
Angebot Aus- und Weiterbildung in Fragen des Datenschutzes	
- Angebot der Datenaufsicht	-
- Auf Anfrage einer Behörde	2[5]
Zusammenarbeit mit anderen Datenschutzbehörden	2
Interne Aufgaben (Organisation, Buchhaltung, Weiterbildung DSB)	8

[5] Hierbei handelt es sich um die Schulung der neuen Kader sowie eine lockere Gesprächsrunde mit Schülerinnen und Schülern im Rahmen einer Projektwoche.