Stadt Zürich
Datenschutzbeauftragter

2016

Geschätzte Leserinnen und Leser

Die Datenschutzstelle der Stadt Zürich freut sich, Ihnen den Bericht für das Kalenderjahr 2016 präsentieren zu können. Wir hoffen, Ihnen mit unseren Ausführungen zur Digitalisierung, zu Bodycam und Schulsozialarbeit, zu Forschungs- und Statistikvorhaben sowie erstmals auch in Form eines kurzen Interviews zur Informationssicherheit einen interessanten Einblick in die vielfältigen Tätigkeiten der Datenschutzstelle geben zu können.

Für Ihr Interesse danken wir Ihnen bestens.

Datenschutzstelle der Stadt Zürich
Marcel Studer, Datenschutzbeauftragter


LÖWENBRÄU
ZÜRICH
Sultana
A.G.

Inhaltsverzeichnis

A) Digitalisierung der Stadtverwaltung

Digitalisierung scheint die Maxime unserer Zeit zu sein. Um den Inhalt des Begriffs «Digitalisierung» näher zu klären, mag es hilfreich sein, eine in einer ePaper-Publikation festgehaltene Aussage des designierten OIZ-Direktors zu zitieren: «Digitalisierung hat zuerst einmal nichts mit Technik zu tun». Dieser negativen Abgrenzung des Begriffs kann aus Sicht des Datenschutzes nur zugestimmt werden. Die digitale Transformation geschieht zwar durch zunehmende Nutzung von Informations- und Kommunikationstechniken sowie digitaler Geräte, Digitalisierung bedeutet aber in erster Linie die Anpassung von Prozessen und Abläufen und damit verbunden auch die Veränderung der Informationsbearbeitung.

Ob es sich bei der Digitalisierung bloss um einen Modebegriff im Sinne des alten Weins in neuen Schläuchen oder doch um einen zukunftsweisenden Erfolgsfaktor handelt, darauf kann an dieser Stelle nicht näher eingegangen werden. Wie dem auch sei, Fakt ist, dass auch in der Zürcher Stadtverwaltung zunehmend Digitalisierungsprojekte lanciert und umgesetzt werden. In welcher facettenreichen Art und Weise dies geschieht und welche datenschutzrechtlichen Fragen sich dabei stellen, sollen die nachfolgenden Vorhaben aus der Verwaltung exemplarisch aufzeigen.

1. Von der Karteikarte zur digitalen Erfassung

Die Auswirkungen, die die Digitalisierung selbst bei scheinbar «einfachen» Vorhaben in datenschutzrechtlicher Hinsicht mit sich bringen kann, werden nicht selten unterschätzt. Vor allem die Annahme, dass mit einer Digitalisierung bzw. einem Einsatz moderner Technologie nicht die Tätigkeit der betreffenden Verwaltungsstelle an sich, sondern nur die Art und Weise der Umsetzung oder der Hilfsmittel ändere und so gesehen ja nichts anderes als bisher gemacht werde, kann dazu führen, dass datenschutzrechtliche Anforderungen zu wenig beachtet werden.

Um zu erkennen, welche datenschutzrechtlichen Aspekte bei einem bestimmten Vorhaben relevant sein können, bedarf es regelmässig einer intensiven Auseinandersetzung mit den Tätigkeiten einer jeweiligen Verwaltungsstelle. Welche gesetzlichen Aufgaben werden erfüllt? Wie geschieht dies? Weshalb geschieht dies so und nicht anders? Solche grundlegenden Klärungen werden bei Vorhaben, die durch neue Aufgaben oder neue Tätigkeiten initiiert werden, in der Regel selbstverständlich durchgeführt. Sie sind aber auch bei Projekten, die bereits bestehende Aufgaben und Tätigkeiten quasi vom Zeitalter der Karteikarten in die digitale Welt transformieren, vorzunehmen. Erst wenn diese Fragen geklärt sind, können Lösungsansätze – insbesondere für die zentrale datenschutzrechtliche Voraussetzung der Verhältnismässigkeit und der sich daraus ergebenden Anforderungen nach Zugriffsregelung oder Datenlöschung – gefunden werden. Stellvertretend für zahlreiche Projekte der Stadtverwaltung soll dies nachfolgend am Beispiel der Einführung einer Softwareapplikation bei der Mütter- und Väterberatung der Sozialen Dienste aufgezeigt werden.

Klärung der Prozesse und Abläufe

Die Mütter- und Väterberatung ist ein Angebot der Sozialen Dienste der Stadt Zürich. In 20 Quartierberatungsstellen beraten und unterstützen Mütter- und VäterberaterInnen Eltern von Babys und Kleinkindern in allen Fragen rund um die Entwicklung, Erziehung und Pflege. Es handelt sich um eines der beliebtesten Angebote der Sozialen Dienste. Jedes Jahr nehmen circa 70% aller Stadtzürcher Eltern, die ein Baby bekommen, das Angebot der Mütter- und Väterberatung in Anspruch.

In der Beratung der Mütter- und VäterberaterInnen können u. a. medizinische Daten sowie Daten betreffend Familienstruktur, Beziehungskonflikte, finanzielle Verhältnisse sowie je nach Fall weitere als sensibel zu qualifizierende Daten bearbeitet werden. Als Bereich der ambulanten Kinder- und Jugendhilfe finden sich die einschlägigen gesetzlichen Grundlagen, die für die Mütter- und Väterberatung gelten, im kantonalen Kinder- und Jugendhilfegesetz. Dieses regelt u. a. die Informationsbeschaffung von Personendaten sowie den Datenaustausch im Bereich der Kinder- und Jugendhilfe. Die datenschutzrechtlichen Herausforderungen dieses Projekts lagen jedoch nicht bei den Themen Datenerhebung oder Datenaustausch, sondern vielmehr bei der Schwierigkeit der Regelung der Zugriffsberechtigungen auf die Daten, der Thematik der Datenlöschung sowie der Gewährleistung von Transparenz gegenüber den betroffenen Eltern.

Zugriffsregelung

Mütter- und Väterberatungsstellen gibt es an verschiedenen Standorten in der Stadt Zürich. Die Beratungsstellen verfügen über jeweils unterschiedliche Öffnungszeiten und Beratungstage. Eltern haben so die Möglichkeit, in der ganzen Stadt eine Beratungsstelle nach

ihrer Wahl und ohne Voranmeldung aufzusuchen, auch ausserhalb des eigenen Sozialraums. Erfahrungsgemäss nutzen denn auch die Eltern die Angebote verschiedener Beratungsstandorte. Neben der Beratung vor Ort bietet die Mütter- und Väterberatung ebenfalls Telefonberatungen an. Auch diese haben je nach Beratungsstandort andere Telefonzeiten und können von allen Eltern genutzt werden.

Damit Eltern jeweils professionell und individuell beraten werden können, ist es wichtig, dass alle BeraterInnen vor Ort oder am Telefon Zugriff auf die für die jeweilige Beratung relevanten Klientendaten haben. Kann dieser Zugriff nicht gewährleistet werden, besteht die Gefahr, dass wichtige, bereits vorhandene Angaben nicht in eine Beratung einfliessen und dies zu einer unbefriedigenden Beratungsqualität führt.

Diese Anforderungen und Bedürfnisse, vor allem hinsichtlich der hohen Flexibilität der Nutzung des Beratungsangebots, waren bei der Zugriffs- und Berechtigungsregelung zu berücksichtigen und führten schliesslich dazu, dass alle BeraterInnen Zugriff auf alle Beratungsdossiers haben. Mit der neuen Applikation können alle BeraterInnen unabhängig von Standort und unabhängig davon, ob es sich um eine Beratung vor Ort oder am Telefon handelt, elektronisch auf alle für sie in der jeweiligen Beratung relevanten Daten zugreifen. Dieser Zugriff erscheint auf den ersten Blick zwar weit, ist aber in Anbetracht der erwähnten Gegebenheiten verhältnismässig und insbesondere für die Erfüllung der gesetzlichen Aufgaben der Mütter- und VäterberaterInnen unentbehrlich.

Datenlöschung

Wie lange müssen Daten in einem System verfügbar sein bzw. wann müssen diese gelöscht werden? Auch die Löschung der Daten bzw.

deren Entfernen aus dem operativen Bereich ist eine Frage der Verhältnismässigkeit und kann nur in Relation zur gesetzlichen Aufgabenerfüllung der jeweiligen Verwaltungsstelle beurteilt werden. Für die Mütter- und Väterberatung wurde eine Frist von 3 Jahren festgelegt. Ein Fall bleibt während drei Jahren nach der letzten Beratung aktiv, weil es aus fachlicher Sicht angezeigt ist, dass bei der Geburt eines weiteren Kindes auf die Akten des älteren Geschwisters zurückgegriffen werden kann. In der Beratung kommt es oft vor, dass Familien, die mit einem Neugeborenen in die Beratung kommen, gleichzeitig auch Fragen zum älteren Geschwister haben. Erfahrungsgemäss folgen Geschwister üblicherweise innerhalb von drei Jahren.

Transparenz

Das Transparenzgebot ist ein datenschutzrechtlicher Grundsatz, welchem bei jeder Datenbearbeitung eine zentrale Bedeutung zukommt. Es spielt insbesondere in jenen Fällen eine grosse Rolle, in welchen eine Einwilligung in die fragliche Datenbearbeitung erteilt werden muss. Werden sensible Informationen bzw. besondere Personendaten bearbeitet, ist das Transparenzgebot so zu gestalten, dass seitens der Verwaltung eine aktive Informationspflicht gegenüber den Betroffenen besteht.

Im vorliegenden Projekt setzten die Sozialen Dienste das Transparenzgebot um, indem in einer internen Weisung eine Aufklärungspflicht gegenüber den betroffenen Eltern festgehalten wurde. So informieren Mütter- und VäterberaterInnen die Eltern anlässlich eines Erstkontakts möglichst adressatengerecht über das Erheben der beratungsnotwendigen Daten und die damit verbundenen Zwecke und Zugriffsmöglichkeiten. Weiter werden die Eltern darüber informiert, dass sie jederzeit Einsicht in die sie betreffenden Akten verlangen können.

2. Das digitale Primat

Immer mehr Verwaltungseinheiten wünschen sich eine moderne und zeitgemässe Form der Erfassung und Verwaltung von Daten und damit die Ablösung von «antiquierten» Papierdokumenten durch ausschliesslich elektronisch geführte Dossiers. Neben den klaren Vorteilen, die die digitale Aktenführung beispielsweise hinsichtlich Verfügbarkeit, Zugriff oder Datenpflege mit sich bringt, gilt es zu beachten, dass im Kontext der Digitalisierung von Dokumenten in rechtlicher Hinsicht diverse Unklarheiten und Unsicherheiten bestehen.

Die Datenschutzstelle hatte im Berichtsjahr zum Thema «digitales Primat» unter anderem ein Projekt zu prüfen, bei dem es um die Einführung rein digital geführter Personaldossiers ging. Die betroffene Dienstabteilung hatte die Absicht, alle analog bestehenden Personaldossiers zu digitalisieren und künftig nur noch in elektronischer Form zu führen. Zudem sollten sämtliche Originalunterlagen nach deren Erfassung vernichtet werden. Nach eingehenden Abklärungen von Seiten der Datenschutzstelle wurde allerdings klar, dass gemäss der derzeit geltenden Rechtslage bestimmte Dokumente nach wie vor im Original physisch aufbewahrt werden müssen. Auf das parallele Führen sogenannter hybrider Dossiers, d. h. Dossiers mit Unterlagen sowohl in Papier- als auch in elektronischer Form, kann daher nicht verzichtet werden.

Im Zusammenhang mit der Umsetzung des digitalen Primats können für die Stadtverwaltung folgende allgemeine Ausführungen gemacht werden:

Form der Dossiers

Massgebend für die Frage, in welcher Form Dossiers einer bestimmten Verwaltungseinheit geführt werden müssen bzw. dürfen, ist in erster Linie die jeweilige Spezialgesetzgebung. So sieht beispielsweise das kantonale Patientinnen- und Patientengesetz vor, dass Patientendokumentationen schriftlich oder elektronisch geführt werden können. Das für die Führung von Personalakten massgebende städtische Personalrecht enthält demgegenüber keine explizite Bestimmung über die Form der Personaldossiers. Aus den Ausführungsbestimmungen ergibt sich jedoch, dass die Regelungen über die Personalakten und Personaldossiers sowie über die Beschaffung, Bekanntgabe und Aufbewahrung von Personendaten auch für elektronisch geführte Datensammlungen gelten. Daraus ist zu schliessen, dass Personaldossiers auch in elektronischer Form geführt werden dürfen.

Beinhaltet die Spezialgesetzgebung keine Vorschriften über die Form von Dossiers, muss geprüft werden, ob allenfalls in Rahmengesetzgebungen wie beispielsweise dem Informations- und Datenschutzgesetz (IDG) diesbezügliche Regelungen zu finden sind. Das IDG bestimmt, dass unter dem Begriff «Informationen» alle Aufzeichnungen unabhängig von Darstellungsform und Informationsträger zu verstehen sind, beinhaltet im Weiteren aber keine spezifische Bestimmungen zur Dossierform. Das IDG äusserst sich also nicht explizit über die Form von Dossiers, sondern hält nur fest, dass die datenschutzrechtlichen Anforderungen unabhängig von der jeweiligen Dossierform auf alle Personendaten anzuwenden sind.

Archivrecht

Die derzeit geltende Fassung der Archivverordnung des Kantons Zürich enthält eine Bestimmung, wonach Akten nach Möglichkeit im Original aufzubewahren sind. Interpretiert man diesen Passus streng, dürfen Originalakten nach einer Digitalisierung nur dann vernichtet werden, wenn dies ausdrücklich in einer gesetzlichen Grundlage erlaubt wird. Es ist derzeit unklar, ob und unter welchen Umständen von einer derart restriktiven Interpretation abgesehen werden kann und somit Originalakten auch ohne explizite Grundlage nur noch in elektronischer Form aufbewahrt werden dürfen. Im Rahmen der anstehenden Revision der kantonalen Archivverordnung wird sich zeigen, ob diese Bestimmung angepasst oder allenfalls sogar vollständig wegfallen wird.

Beweiskraft elektronischer Unterlagen

Bei der rein elektronischen Führung eines Dossiers stellt sich die Frage nach der Beweiskraft eingescannter Dokumente. Im Streitfall (z. B. Geltendmachung von Forderungen, Haftpflicht- oder Strafverfahren vor Gericht) haben Originalurkunden bzw. Urkunden mit originalen Unterschriften einen höheren Beweiswert als eingescannte, kopierte und anschliessend ausgedruckte Dokumente. Das Bundesgericht hat dazu in einem Urteil vom August 2015 ausgeführt, dass nur anhand eines Originals (und somit ausdrücklich nicht anhand einer Kopie oder eines Scans) erhobene Befunde eine positive Urheberaussage begründen können und der Nachweis der Echtheit einer Fotokopie nicht möglich sei. Dies bedeutet, dass bestimmte Originalunterlagen mit handschriftlicher Unterschrift nach dem Einscannen weiterhin in Papierform aufbewahrt werden sollten. Geltung hat das insbesondere für jene Dokumente, für die aufgrund der damit verbundenen Rechtsansprüche das Erfordernis der Unterschrift besteht. Zusätzlich zum

Risiko der Beweislosigkeit sind auch allfällige Reputationsrisiken der Verwaltung mit zu berücksichtigen. Jede betroffene Verwaltungseinheit muss daher diesbezügliche Risikoabwägungen durchführen und festlegen, welche Originalunterlagen weiterhin auf Papier aufbewahrt werden. Dies können beispielsweise folgende Kategorien von Unterlagen betreffen:

- Verträge
- Personalrechtliche Massnahmen / Verwarnungen
- Unterlagen aus der Verwaltungsrechtspflege
- Eingeschriebene Briefe
- Arztzeugnisse

Elektronische Signatur

Der Einsatz einer qualifizierten elektronischen Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten beruht und dadurch gemäss Bundesrecht der eigenhändigen Unterschrift gleichgesetzt ist, ermöglicht es grundsätzlich, auf Papierunterlagen zu verzichten. Von Gesetzes wegen gibt es denn auch nur sehr wenige Konstellationen, bei denen die eigenhändige Unterschrift nicht durch eine qualifizierte elektronische Signatur ersetzt werden könnte (dies ist beispielsweise bei eigenhändigen letztwilligen Verfügungen der Fall).

In der Praxis hat sich die elektronische Signatur bis heute jedoch kaum durchgesetzt und ihre Verbreitung schreitet nur langsam voran. Gründe für den mangelnden Einsatz der elektronischen Signatur sind die mit ihr verbundenen technischen Herausforderungen und die hohen Kosten. Auch mangelt es der elektronischen Signatur an Praktikabilität. So müssen nicht nur Personen innerhalb einer Ver-

waltungseinheit, sondern auch allfällige Dritte über eine elektronische Signatur verfügen (beispielsweise Ärzte, die Zeugnisse verfassen oder Personen, mit denen ein Vertrag abgeschlossen werden soll). Kaum vielversprechend scheint der Einsatz der elektronischen Signatur auch dann zu sein, wenn bereits bestehende Originaldokumente digitalisiert werden. Denn diese müssten ebenfalls – soweit dies überhaupt möglich wäre – nachträglich mit einer elektronischen Unterschrift versehen werden.

Fazit

Aus dem Gesagten ergibt sich, dass von einer rein elektronischen Führung von (Personal-)Dossiers bei gleichzeitiger Vernichtung der Originaldokumente klar abzuraten ist. Auch wenn sich eine Verwaltungseinheit für das digitale Primat entscheidet, wird es unter Umständen Unterlagen geben, die aus rechtlichen Überlegungen physisch abgelegt und aufbewahrt werden müssen. Die Frage, ob originale Dokumente aufbewahrt werden müssen oder vernichtet werden dürfen, lässt sich nicht in erster Linie aus dem Datenschutzrecht, sondern aus der bereichsspezifischen Spezialgesetzgebung sowie dem Archiv- und Beweisrecht beantworten.

Das Kompetenzzentrum Records Management der Stadt Zürich erarbeitet derzeit für die Stadtverwaltung einen Leitfaden zum Thema «Rechtssicherheit von digitalen Unterlagen». Darin soll aufgezeigt werden, welche grundsätzlichen Überlegungen anzustellen sind, wenn eine Organisationseinheit sich für das digitale Primat entscheidet, gleichzeitig aber auch rechtlich relevante Unterlagen bewirtschaften muss. Der Leitfaden soll voraussichtlich bis Ende 2017 fertiggestellt und veröffentlicht werden. Die Datenschutzstelle ist an der Erarbeitung des Leitfadens beteiligt.


el langstrasse
welcome
sleep
hug
NENI
Zürich
surprise

3. Bürgerkonto

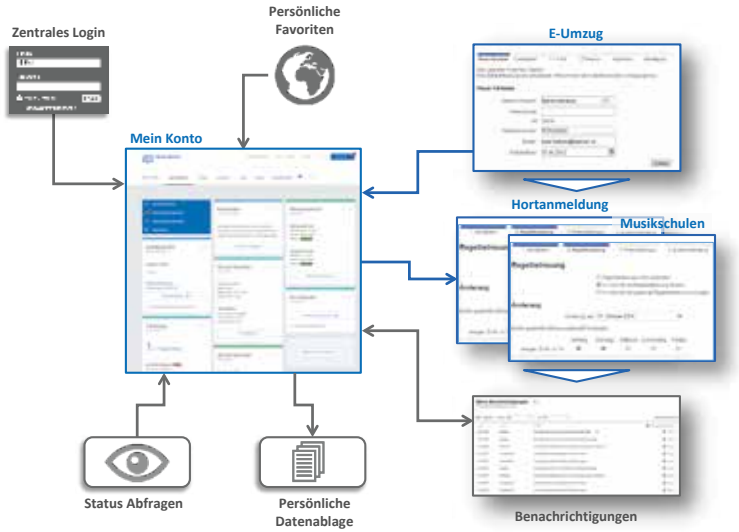
Die Digitalisierung verändert nicht nur interne Verwaltungsprozesse, sondern wirkt sich auch auf die Kommunikation zwischen Verwaltung und BürgerInnen aus. Bereits heute ist der 24-Stunden-Online-Schalter für gewisse Verwaltungsgeschäfte der Stadtverwaltung Realität: Man denke etwa an die elektronischen Umzugsmeldungen innerhalb der Stadt Zürich (E-Umzug), an die Online-Bestellung von Parkkarten oder die Online-Reservation von Heiratsterminen (E-Heirat). Ein neues Vorhaben der Stadt Zürich, welches sowohl den Bürgerinnen und Bürgern, als auch der Stadtverwaltung das Leben künftig erleichtern soll und durchaus als Meilenstein auf dem Weg zum «digitalen Stadthaus» betrachtet werden kann, ist das Projekt «Mein Konto».

«Mein Konto» – das Online-Konto der Stadt Zürich für Bevölkerung und Unternehmen

Schon bald soll in der Stadt Zürich den Bürgerinnen und Bürgern ein Online-Konto zur Verfügung stehen, über welches sie wichtige Verwaltungsgeschäfte bequem von zu Hause oder unterwegs über Tablet oder Handy abwickeln und sich Informationen aus der Stadtverwaltung nach eigenen Bedürfnissen zusammenstellen können. Die Stadt Zürich hat im E-Government bereits früh eine Vorreiterrolle übernommen, wie die eingangs erwähnten Online-Dienste zeigen. Auch hat die Stadt Zürich ihren Internetauftritt auf die Informationsbedürfnisse ihrer Bürgerinnen und Bürger ausgerichtet. Was bis heute fehlt, ist ein zentrales, «digitales Eingangstor» zum gesamten E-Government-Angebot der Stadtverwaltung. Nach wie vor ist es recht mühsam und zeitaufreibend, sich im virtuellen Verwaltungsdschungel zurecht zu finden, da die Zugänge zu den einzelnen E-Government-Angeboten dezentral über die Dienstabteilungen er-

folgen und die Nutzung der Online-Dienste zum Teil unterschiedlichen Standards (bspw. unterschiedliche Registrierungsprozesse) folgen. «Mein Konto» wird in Zukunft das zentrale Eingangstor zum städtischen E-Government-Angebot sein. Es übernimmt dabei die Aufgabe der Zugangskontrolle, ist aber auch Wegweiser, persönliches Informationsbrett, Posteingang und vieles mehr.

«Mein Konto»



Datenschutzrechtliche Schwerpunkte

Die Realisierung eines Online-Kontos berührt auch den Datenschutz. Die Datenschutzstelle stand schon zu Beginn des Projekts in regelmässigem Kontakt mit der Projektleitung und achtete beim Aufbau des Online-Kontos für die Bürgerinnen und Bürger auf die Einhaltung der datenschutzrechtlichen Anforderungen. Dabei war von Anfang an klar, dass eine generische Prüfung von «Mein Konto» nur sehr beschränkt möglich ist, da eine solche Prüfung von den einzelnen Online-Diensten abhängt, welche in «Mein Konto» eingebunden werden. Die folgenden Themen zeigen, wo bei «Mein Konto» die datenschutzrechtlichen Schwerpunkte liegen.

– «Mein Konto» gehört den Bürgerinnen und Bürgern

  Das Online-Portal «Mein Konto» ist ein freiwilliges Angebot der Stadt an die Bürgerinnen und Bürger. In «Mein Konto» können die Nutzenden ganz nach ihren Bedürfnissen aus der Vielzahl der eingebundenen Anwendungen ihre Favoriten auswählen und so ihr Konto persönlich gestalten. Da schon die Gestaltung eines solchen Kontos Hinweise auf die Interessen einer Person geben kann, setzt die datenschutzrechtliche Relevanz bereits hier an: das Konto gehört den Bürgerinnen und Bürgern und nur sie bestimmen über ihre Daten. Die Stadt soll grundsätzlich keinen Zugang zum personalisierten Konto der jeweiligen Personen erhalten. Ausnahmen sind möglich bei Supportanfragen oder bei allfälligen technischen Störungen.

– Informationelle Trennung

  In «Mein Konto» werden unterschiedliche Serviceangebote der Dienstabteilungen eingebunden: beispielsweise Anmeldungen zum Musikschulunterricht bei der Musikschule Konservatorium Zürich, Umzugsmeldungen beim Personenmeldeamt, Bestel-

lungen von Parkkarten bei der Dienstabteilung Verkehr oder Betreuungsanmeldungen bei einem Hort. Dabei muss sichergestellt sein, dass die Dienstabteilungen nur Zugang zu denjenigen Personendaten haben, welche das eigene Serviceangebot bzw. die eigenen Geschäftsprozesse betreffen. Sollen künftig E-Government-Anwendungen in «Mein Konto» eingebunden werden, welche einen elektronischen Informationsaustausch über diese Grenzen hinaus erfordern (zu denken ist etwa an Bewilligungsverfahren, an welchen mehrere Dienstabteilungen beteiligt sind), ist dies, wie bei allen Bekanntgaben von Personendaten, nur gestützt auf entsprechende Rechtsgrundlagen oder mit Einwilligung der betroffenen Personen zulässig.

– Authentifizierung

  Die Anmeldung in «Mein Konto» erfolgt über ein Log-in mittels Benutzername und Passwort, ohne dass sich die Nutzenden genauer identifizieren müssen. Damit soll ein niederschwelliger Zugang zu «Mein Konto» möglich sein. Für den Zugang zu rein informativen, nicht sensiblen Online-Diensten (beispielsweise die Nutzung eines Abfall- oder Ferienkalenders) genügt eine solch schwache Authentisierung. Für die Nutzung von Online-Diensten, bei welchen verbindliche oder kostenpflichtige Geschäftsprozesse ausgelöst werden können oder welche die Bearbeitung von (sensiblen) Personendaten beinhalten, genügt eine solche Authentisierung mittels Benutzername und Passwort nicht. Welche Authentisierungsmassnahmen konkret umzusetzen sind, hängt vom Schutzbedarf des jeweiligen Online-Dienstes, aber auch von der Praktikabilität für die Nutzenden ab. So können weitere Identitätsabklärungen und zusätzliche Eingabecodes beim Log-in (beispielsweise ein zusätzlicher SMS-Code) notwendig sein.

– Sichere Zuordnung von Daten zu einer bestimmten Person

  Die Dienstabteilungen setzen für die Abwicklung ihrer Verwaltungsgeschäfte verschiedene Fachanwendungen ein. In diesen Systemen werden die geschäftsrelevanten Personendaten der Bürgergerinnen und Bürger gespeichert. Soll nun ein Geschäftsprozess online abgewickelt werden, muss die Fachanwendung direkt in den Online-Service eingebunden sein. Dabei muss sichergestellt sein, dass die persönlichen Informationen aus der Fachanwendung auch wirklich denjenigen Personen zugeordnet werden, welche einen Online-Service in Gang setzen. Dies geschieht technisch über eindeutige Identifikatoren (wie AHV-Nummer, Schülernummer oder dergleichen). In «Mein Konto» wurde hierfür ein sogenannter fachlicher Schlüsselbund eingebaut. Dieser ist das Bindeglied zwischen «Mein Konto» und den Fachanwendungen und enthält die für die erwähnte Zuordnung notwendigen Identifikatoren. Die Konzeption des fachlichen Schlüsselbundes erfolgt nach dem schweizweiten E-Government-Standard eCH-0107 (Gestaltungsprinzipien für Identitäts- und Zugriffsverwaltung).

– Sichere Kommunikation

  Trotz technischer Fortschritte in den letzten Jahren besteht in der Stadtverwaltung nach wie vor keine flächendeckende, einfache und gleichzeitig sichere E-Mail-Kommunikationsmöglichkeit zwischen den Amtsstellen und den Bürgerinnen und Bürgern. Zwar gibt es entsprechende Kommunikationsplattformen von Drittanbietern, diese Dienste sind aber eher schwerfällig und werden von Privatpersonen kaum genutzt. «Mein Konto» kann hier Abhilfe schaffen, da es eine sichere Kommunikation zwischen den Kontonutzenden und den Amtsstellen ermöglicht.

– Wiederverwendbarkeit von Stammdaten
  Ein lästiges Thema für die Bürgerinnen und Bürger ist das Ausfüllen amtlicher Formulare. In diesen werden immer wieder die gleichen Angaben wie Name, Adresse, Wohnort, Geburtsdatum, Telefonnummer etc. verlangt. Mit «Mein Konto» soll nun für die Bürgerinnen und Bürger eine Erleichterung geschaffen werden: Die in «Mein Konto» bei der Registrierung erfassten und jederzeit durch die Inhaberinnen und Inhaber des Kontos aktualisierbaren Stammdaten können für das Service-Angebot von «Mein Konto» wiederverwendet werden. Die Stammdaten können automatisch in ein amtliches Formular übernommen werden. Diese Möglichkeit führt auch zu einer Verbesserung der Datenintegrität, da Fehleingaben (vor allem auf Formularen) vermieden werden können.

– Persönliche Datenspeicherung
  Bei der Nutzung der in «Mein Konto» bereitgestellten Online-Dienste können Informationen anfallen, über welche die Bürgerinnen und Bürger selber bestimmen, ob und wo sie diese speichern wollen. Die Datenspeicherung erfolgt damit getrennt vom städtischen System «Mein Konto». Dies verhindert, dass eine zentrale Sammlung von persönlichen Daten der Bürgerinnen und Bürger auf der städtischen Infrastruktur entsteht.

Ausblick

Während «Mein Konto» sich auf städtischer Ebene bewegt, sind Bestrebungen des Bundes im Gange, gewisse Grundanforderungen auf nationaler Ebene zu lösen. Die im Schwerpunktplan 2017–2019 von E-Government Schweiz definierten operativen Ziele nennen ein für die ganze Schweiz einheitliches Anmeldeverfahren für E-Government-Dienste auf Portalen verschiedener föderaler Ebenen, die Eta-

blierung einer national und international gültigen elektronischen Identität (E-ID) oder die schweizweite und medienbruchfreie elektronische Meldung von Weg- und Zuzügen. Die E-Government-Aktivitäten des Bundes werden damit einen massgebenden Einfluss auf die Aktivitäten der Stadt und insbesondere auf «Mein Konto» haben. Beim Ausbau und der Umsetzung von «Mein Konto» müssen daher stets die Aktivitäten und Standards des Bundes in die Planung auf städtischer Ebene einbezogen werden. Gleichzeitig werden Aktivitäten auf Seiten Schweizer Städte und Gemeinden auch in Projekte auf Ebene des Bundes und der Kantone einbezogen. Letztlich erfordern diese ebenenübergreifenden Abhängigkeiten und Aktivitäten der Behörden auch eine aktive Zusammenarbeit der Datenschutzstellen.


ZURICH

4. Die AHV13-Nummer: Identifikator contra legem?

Seit einigen Jahren bietet das Zivilstandsamt der Stadt Zürich die Anwendung E-Heirat zur einfachen und schnellen Online-Reservation von Heiratsterminen an. Dabei ist das Zivilstandsamt für die Terminreservation auf korrekte und eindeutige Informationen angewiesen. Fehlerhafte Anmeldungen, Flüchtigkeitsfehler oder mehrfach vorkommende, identische Namen machen es teilweise schwierig, die Identität einer Person eindeutig festzustellen. Um solche Identifizierungsprobleme zu beheben sowie zur Effizienzsteigerung interner Prozesse, wollte das Zivilstandamt im Berichtsjahr die AHV-Versichertennummer der sich anmeldenden Personen als eindeutigen Identifikator im Anmeldungsprozess verwenden und bat die Datenschutzstelle um eine diesbezügliche Prüfung.

Die AHV13-Nummer: Theorie und Praxis

Die «neue», heute geltende 13-stellige AHV-Versichertennummer wurde vor knapp zehn Jahren in der Schweiz eingeführt. Sie ersetzte die alte 11-stellige AHV-Nummer, welche u. a. aus Sicht des Datenschutzes problematisch war. Anhand der AHV-Nummer konnte man nämlich das Geburtsdatum, das Geschlecht und die Anfangsbuchstaben des Namens einer Person bestimmen. Dieses Problem konnte mit Einführung der neuen AHV-Nummer behoben werden. So ist die neue 13-stellige Nummer im Gegensatz zu ihrer Vorgängerin «nicht sprechend» und zufällig generiert.

Die Verwendung der neuen AHV13-Nummer wird ausführlich im Bundesgesetz über die Alters- und Hinterlassenenversicherung ge-

regelt. Dort ist festgehalten, dass jede systematische Verwendung der AHV13-Nummer ausserhalb des Sozialversicherungsrechts einer gesetzlichen Grundlage (auf Stufe Bund oder Kanton) bedarf und der Zentralen Ausgleichsstelle gemeldet werden muss. Dieser Gesetzesvorbehalt wurde ursprünglich eingeführt, um zu erreichen, dass die Verbreitung der AHV13-Nummer ausserhalb des Sozialversicherungsbereichs minimal bleibt bzw. die Verwaltungsbereiche, welche mit dieser Nummer arbeiten, auf einen kleinen Kreis beschränkt werden.

Anders als vom Gesetzgeber ursprünglich vorgesehen verwenden heute eine Vielzahl von Behörden sämtlicher föderalen Ebenen sowie auch private Institutionen die AHV13-Nummer als eindeutigen Personenidentifikator in ihren Fachapplikationen. Die Versichertennummer wird heute bereits landesweit für Meldungen von Gesundheitsdaten, bei der Durchführung der privaten Zusatzversicherungen, im Bildungswesen, im Asylbereich sowie zum Eintreiben der Billag-Gebühren verwendet. Auch ins Ausland wird die AHV13-Nummer geschickt, seit sie im Rahmen des automatischen Informationsaustauschs als Steueridentifikationsnummer dient. Diese Beispiele zeigen, dass eine stetig zunehmende Verwendung der AHV13-Nummer durch die Bundesverwaltung, kantonale und kommunale Verwaltungen sowie Private stattfindet und die ursprüngliche Idee, diese Nummer nur in wenigen Bereichen der Verwaltung einzusetzen, zumindest faktisch überholt scheint. Die Zentrale Ausgleichstelle verwaltet ein Verzeichnis der Institutionen, welche sich bei ihr als systematische Benutzer der AHV13-Nummer melden. Dieses öffentlich zugängliche Verzeichnis zählt heute über 10 000 systematische Benutzer und veranschaulicht auf eindrückliche Weise die weite Verbreitung der AHV13-Nummer.

Datenschutzrechtliche Kritik und neueste Entwicklungen

Die breite Verwendung der Versichertennnummer wird von Datenschützern kritisiert. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist der Ansicht, dass durch den Einsatz eines bereichsübergreifenden Personenindentifikators eine missbräuchliche Verwendung von personenbezogenen Daten technisch erleichtert werde. Zudem bestehe die erhebliche Gefahr, dass über die AHV13-Nummer Verknüpfungsmöglichkeiten entstehen (oder doch zumindest nicht ausgeschlossen werden können), die sich unter dem Aspekt des verfassungsrechtlichen Persönlichkeitsschutzes als höchst problematisch erweisen könnten.

Trotz dieser Kritik aus datenschutzrechtlicher Sicht möchte der Bundesrat aus der AHV13-Nummer eine behördenweite Identifikationsnummer für sämtliche EinwohnerInnen machen. Er hat dem Departement des Inneren den Auftrag erteilt, bis im Herbst 2017 eine Gesetzesvorlage auszuarbeiten, welche es allen Behörden von Bund, Kantonen und Gemeinden erlaubt, die AHV13-Nummer systematisch zur Personenidentifikation einzusetzen. Dies vor allem mit der Begründung, dass dadurch Verwaltungsabläufe effizienter gestaltet werden können.

In zahlreichen Verwaltungsabläufen besteht bereits heute das Erfordernis, BürgerInnen bzw. KundInnen eindeutig zu identifizieren. Mit zunehmender Digitalisierung der Verwaltung und vermehrtem Einsatz von Online- bzw. E-Government-Applikationen wird der Bedarf nach eindeutigen Personenidentifikatoren in Zukunft eine immer wichtigere Rolle spielen. Da die AHV13-Nummer die einzige Nummer ist, welche die gesamte Wohnbevölkerung in der Schweiz durch die Vergabe einer eindeutigen Nummer erfasst, ist davon auszugehen, dass diese als eindeutiger Personenidentifikator auch in Zukunft hoch im Kurs

sein wird. Inwiefern die Verwaltung die AHV13-Nummer als eindeutige Identifikationsmöglichkeit verwenden darf, wird der Ausgang der aktuellen politischen Debatte zeigen müssen.

Verwendung der AHV13-Nummer in E-Heirat

Vor diesem Hintergrund prüfte die Datenschutzstelle den Wunsch des Zivilstandsamts, die AHV13-Nummer im Anmeldungsprozess von E-Heirat zu verwenden. Aufgrund der Zivilstandsverordnung ist das Zivilstandsamt berechtigt (bzw. verpflichtet), die AHV13-Nummer systematisch im Zivilstandsregister zu führen. Wenn nun eine sich über E-Heirat anmeldende Person ihrerseits die AHV13-Nummer in diese Applikation eingibt, ermöglicht sie dem Zivilstandsamt einen Abgleich über diesen eindeutigen Identifikator und bei einer Übereinstimmung eine eindeutige Identifizierung der Person. Die Verwendung der AHV13-Nummer in der Applikation E-Heirat dient einzig der internen Organisation des Zivilstandsamts und wird in der Zusammenarbeit mit Dritten oder Behörden weder benötigt noch genannt. Die Eingabe der AHV13-Nummer, welche für den Abgleich bzw. zur eindeutigen Identifikation getätigt wird, erfolgt durch die Anmeldenden freiwillig. Diese können auf diese Angabe verzichten, ohne dass der Anmeldeprozess für sie dadurch beeinträchtig würde. Die von den Anmeldenden eingegebene Nummer wird nicht gespeichert, sondern nach erfolgtem Abgleich durch das Zivilstandsamt wieder gelöscht. Die Datenschutzstelle erachtet diese Verwendung der AHV13-Nummer in der Applikation E-Heirat durch das Zivilstandsamt als rechtskonform und verhältnismässig.

B) Prinzip der Gesetzmässigkeit

Massstab und Schranke der Verwaltungstätigkeit ist das Gesetz. Das Handeln der Verwaltung hat somit auf Rechtsgrundlagen zu beruhen. Dieses Erfordernis nach genügenden gesetzlichen Grundlagen verlangt das Gesetzmässigkeit- bzw. Legalitätsprinzip, welches in der Schweizerischen Bundesverfassung verankert ist. Die Datenschutzgesetzgebungen konkretisieren dieses allgemeine Verfassungsprinzip mit Bezug auf die Datenbearbeitung durch die Verwaltung und verlangen – so wie beispielsweise das IDG des Kantons Zürich – für das Bearbeiten von sensiblen Personendaten hinreichend bestimmte Regelungen in einem formellen Gesetz.

Das Prinzip der Gesetzmässigkeit ist im datenschutzrechtlichen Alltag der öffentlichen Verwaltung von zentraler Bedeutung. Ob und welche Personendaten von Verwaltungsstellen erhoben, bearbeitet und mit anderen Stellen ausgetauscht werden dürfen, bemisst sich stets nach der Bereichsgesetzgebung der jeweiligen Verwaltungstätigkeiten. Beabsichtigt eine Vewaltungsstelle, sensible Personendaten in einem Umfang oder in einer Art und Weise zu bearbeiten, wie sie es bis anhin noch nicht getan hat, steht zu Beginn eines solchen Vorhabens auf alle Fälle eine detaillierte Prüfung der Rechtsgrundlagen im Vordergrund. Das nachfolgende Beispiel des Pilotprojekts «Bodycam» soll dies veranschaulichen. Aber nicht nur bei Einführung neuer Aufgaben oder Datenbearbeitungen kann die Auseinandersetzung mit den gesetzlichen Grundlagen im Fokus stehen. Unter Umständen zeigt sich auch bei Verwaltungstätigkeiten, die bereits schon seit geraumer Zeit praktiziert werden, dass genügend bestimmte Rechtsgrundlagen fehlen. Fragen nach einem korrekten Umfang mit sensiblen Personendaten können in solchen Fällen regelmässig nur schwierig beantwortet werden. Das Beispiel der Schulsozialarbeit verdeutlicht dies.

1. Bodycam

Bodycams – zu Deutsch Körperkameras bzw. auf dem Körper getragene Kameras – waren bis anhin vor allem in den USA bekannt. Während sie dort dem Schutz der Bürgerinnen und Bürger vor gewalttätigen Übergriffen polizeilicher Einsatzkräfte dienen, werden sie hierzulande in erster Linie als eine Massnahme gegen die zunehmende Gewalt an Polizistinnen und Polizisten gesehen. Mit der Mitteilung der Stadtpolizei vor gut einem Jahr, sie werde aufgrund der stets zunehmenden Übergriffe auf ihre Mitarbeitenden den Einsatz von Bodycams prüfen, war über Zürich hinaus eine kontroverse Debatte lanciert. Bei diesem Vorhaben der Stadtpolizei war die Datenschutzstelle von Beginn an involviert und das Projekt Bodycam wurde für sie zum aufwendigsten Geschäft des Berichtsjahres.

Die (fehlenden) Grundlagen im kantonalen Polizeirecht

Mit einem Einsatz von Bodycam erhebt die Polizei Ton- und Bilddaten und greift dadurch in die Grundrechte betroffener Personen ein. Die Frage, ob die Polizei dazu berechtigt ist, hat sich aus dem für die Stadtpolizei massgebenden Polizeirecht zu ergeben.

– Keine Überwachungsmassnahme im eigentlichen Sinne
  Das Polizeigesetz des Kantons Zürich erlaubt der Polizei unter dem Titel «Überwachungsmassnahmen», bei Grossveranstaltungen und Kundgebungen oder ausserhalb derartiger Veranstaltungen einzelfallweise und auf Anordnung hin öffentlich zugänglichen Raum mit Audio- und Videogeräten zu überwachen. Obwohl auch ein Einsatz von Bodycam im Endeffekt ein Aufzeichnen von Bild und Ton bei Polizeieinsätzen beinhaltet und schliesslich auch eine gewisse Überwachung mit sich bringt, waren sich Stadtpolizei,

Sicherheitsdepartement und Datenschutzstelle einig, dass Bodycam dennoch keine eigentliche Überwachungsmassnahme im Sinne des kantonalen Polizeigesetzes darstellt und deshalb nicht unter die diesbezüglichen Videoüberwachungen subsumiert werden kann.

– Prävention und Dokumentation

  Mit dem Einsatz von Bodycam sollte nicht in erster Linie eine weitere Überwachungsmassnahme des öffentlichen Raums eingeführt werden, sondern vielmehr erreicht werden, dass Eskalations- und strafbares Verhalten bei bestimmten Polizeieinsätzen nach Möglichkeit verhindert oder – falls dies nicht erreicht werden kann – mindestens dokumentiert wird. Gemäss kantonalem Polizeigesetz ist die Stadtpolizei berechtigt, Personenkontrollen durchzuführen. Diese hat sie angemessen zu dokumentieren, was in der Regel mit einer entsprechenden Protokollierung geschieht. Der Einsatz von Bodycam basiert auf diesen polizeilichen Aufgaben gemäss kantonalem Polizeigesetz und bezweckt, die Dokumentation bestimmter Anhaltungen oder Kontrollen mit Ton- und Bildaufnahmen zu ergänzen.

– Fehlende Bestimmtheit der Datenbearbeitung

  Bereits bestehende polizeiliche Aufgaben gemäss kantonalem Polizeigesetz sind also Ausgangspunkt für den Einsatz von Bodycam. Aber weshalb genügen diese Grundlagen nicht, um einen Einsatz von Bodycam zu rechtfertigen? Die Begründung liegt darin, dass das kantonale Polizeirecht zwar Personenkontrolle und Dokumentationspflicht vorsieht, sich aber zur hierfür zulässigen Datenerhebung und Datenbearbeitung nicht äussert. Eine Dokumentation mittels Audio- und Bildaufnahmen tangiert die betroffenen Personen ungleich schwerer als eine blosse Protokollierung und erreicht eine Grundrechtsrelevanz, die nach Grundlagen ver-

langt, welche in genügend bestimmter Weise Voraussetzungen und Modalitäten umschreiben. Derartige Grundlagen finden sich im kantonalen Polizeirecht nicht, sie können aber – gestützt auf die kommunale Kompetenz zum Erlass polizeilicher Vorschriften – von der Stadt Zürich für die Stadtpolizei erlassen werden.

Das Bodycam-Reglement der Stadt Zürich

Um die verlangte genügende Bestimmtheit zu gewährleisten, mussten die wesentlichen Voraussetzungen und Modalitäten für den Einsatz von Bodycam und die sich daraus ergebenden Datenbearbeitungen in klarer, transparenter und verbindlicher Weise geregelt werden. Der Stadtrat hat hierfür im Dezember 2016 ein Reglement über den Pilotversuch Bodycam bei der Stadtpolizei erlassen, welches am 1. Februar 2017 in Kraft getreten ist. Dieses Reglement erfüllt die datenschutzrechtlichen Anforderungen. Hervorzuheben sind dabei insbesondere folgende Regelungen:

Bodycams dürfen nur bei Anhaltungen oder Kontrollen eingesetzt werden, bei welchen gewalttätige oder verbale Übergriffe drohen *(sachlicher Anwendungsbereich).* Der Einsatz von Bodycam hat sich auf entsprechende neuralgische Örtlichkeiten und auf den öffentlichen zugänglichen Raum zu beschränken *(räumlicher Anwendungsbereich).* Mit Bodycams sollen primär Übergriffe verhindert werden. Kann eine präventive Verhinderung nicht erreicht werden, soll die Stadtpolizei den Eskalationsverlauf und das Verhalten der Beteiligten dokumentieren können *(Zweck).* Bodycam darf kein einseitig polizeiliches Instrument darstellen, weshalb auch betroffene Privatpersonen die Aufzeichnung verlangen können und die Polizei zur ganzheitlichen und objektiven Erfassung der Vorfälle verpflichtet ist *(Waffengleichheit).* Ein Einsatz von Bodycam muss für Betroffene erkennbar sein,

weshalb eine entsprechende Kennzeichnung kameraführender Polizeiangehöriger sowie die Ankündigung und die Sichtbarmachung von Aufzeichnungen verlangt werden *(Transparenz).* Die Stadtpolizei hat sicherzustellen, dass Aufnahmen nicht verändert werden und nur Berechtigte Zugriff erhalten *(Integrität und Vertraulichkeit).* Sämtliche Zugriffe sind zu protokollieren *(Nachvollziehbarkeit)* und Aufnahmen sind nach 100 Tagen automatisch zu löschen *(Datenlöschung).*

Reglementierte Pilotversuche gemäss städtischer Datenschutzverordnung

Mit dem Reglement über den Pilotversuch Bodycam hat der Stadtrat zum ersten Mal von einer gesetzgeberischen Möglichkeit Gebrauch gemacht, welche ihm seit dem Jahre 2011 zur Verfügung steht: Dem sogenannten reglementierten Pilotversuch gemäss städtischer Datenschutzverordnung.

– «Experimentelle Gesetzgebung»
  Mit der Totalrevision der städtischen Datenschutzverordnung hat der Gemeinderat dem Stadtrat die Kompetenz eingeräumt, in Ausnahmefällen eine temporäre Rechtsgrundlage zu schaffen, für deren Erlass eigentlich der Gemeinderat zuständig ist. Dieses gesetzgeberische Instrument war bereits aus der Datenschutzgesetzgebung des Bundes bekannt und wurde zwischenzeitlich auch von den Kantonen Basel-Stadt und Aargau in ihre Datenschutzgesetze übernommen. Die Problematik, die zur Einführung derartiger reglementierter Pilotversuche geführt hat, ist folgende: Verfassung und Datenschutzgesetzgebung verlangen von der Verwaltung, dass sie sensible Personendaten erst bearbeitet, wenn die zuständige Legislative hierfür genügend bestimmte Rechtsgrundlagen erlassen hat. Verlangt wird somit, dass ein

Gesetzgebungsprozess so frühzeitig initiiert wird, dass sich die Datenbearbeitungen von Beginn an auf detaillierte Rechtsgrundlagen abstützen können. Insbesondere bei neuen Aufgaben oder dem Einsatz neuer Mittel kann dies zu Schwierigkeiten führen, wenn deren Umsetzung oder Handhabung und damit verbunden auch die daraus resultierenden Datenbearbeitungen erst erprobt werden müssen. Mit dem Instrument der reglementierten Pilotversuche soll der Schwierigkeit Rechnung getragen werden, dass präzise Regelungen unter Umständen erst nach einer gewissen Erfahrungszeit bzw. Versuchsphase geschaffen werden können. Die reglementierten Pilotversuche werden daher auch als «experimentelle Gesetzgebung» bezeichnet.

Die Voraussetzungen, die der Gemeinderat für solche reglementierte Pilotversuche in der städtischen Datenschutzverordnung statuiert hat, sind nach Ansicht der Datenschutzstelle im Falle von Bodycam erfüllt. Zu erwähnen ist vor allem die Anforderung, wonach die praktische Umsetzung der Datenbearbeitung eine Testphase zwingend erfordert. Im Rahmen der Erarbeitung des Reglements über den Pilotversuch Bodycam zeigte sich deutlich, dass ohne Erfahrungswert aus der Praxis zu viele faktische Ungewissheiten und Variablen bestehen würden, um einen für die Stadt Zürich «passenden» Einsatz von Bodycam bestimmen zu können. Um schliesslich die Erfahrungen aus der Versuchsphase auch korrekt interpretieren zu können, lässt die Stadtpolizei das Pilotprojekt Bodycam wissenschaftlich durch die Zürcher Hochschule für angewandte Wissenschaften begleiten.

– Zeitliche Befristung auf maximal 4 Jahre

  Spätestens innerhalb von zwei Jahren seit Beginn des Pilotprojekts muss die Stadtpolizei dem Stadtrat und der Datenschutzstelle einen Evaluationsbericht vorlegen. Gestützt auf diesen Be-

richt kann der Stadtrat das Pilotprojekt um weitere zwei Jahre fortführen lassen. Die städtische Datenschutzverordnung limitiert das Pilotprojekt Bodycam auf längstens vier Jahre. Sollen Bodycams dauerhaft eingeführt werden, muss spätestens nach vier Jahren seit Beginn des Pilotprojekts eine entsprechende rechtliche Grundlage vorhanden sein. Wenn bis dahin der kantonale Gesetzgeber keine Rechtsgrundlage für den Einsatz von Bodycam mit Geltungsbereich für die Gemeinden erlassen wird, liegt es am Gemeinderat, ob für die Stadtpolizei eine solche Grundlage im städtischen Polizeirecht geschaffen werden soll. Haben vier Jahre nach Beginn des Pilotversuchs weder die kantonale noch die städtische Legislative eine rechtskräftige Grundlage zu Bodycam geschaffen, muss die Stadtpolizei den Einsatz von Bodycam und die damit verbundene Datenbearbeitung abbrechen.

2. Schulsozialarbeit

Im September 2002 haben die Stimmbürgerinnen und Stimmbürger der Stadt Zürich beschlossen, die Schulsozialarbeit in den Volksschulen der Stadt Zürich definitiv einzuführen. Heute stehen in rund 100 Schulhäusern der Stadt Schulsozialarbeiterinnen und Schulsozialarbeiter Kindern, Jugendlichen, Eltern, Lehrkräften und Schulbehörden mit Rat und Tat zur Verfügung.

Die Schulsozialarbeit versteht sich als Handlungsfeld der Jugend- und Familienhilfe und wird in der Stadt Zürich als Kooperationsmodell zwischen dem Schul- und Sportdepartement und dem Sozialdepartement geführt. Sie verfolgt das Ziel, Kinder und Jugendliche im Prozess des Erwachsenwerdens zu begleiten und sie bei der Lebensbewältigung zu unterstützen. Der Schwerpunkt der Schulsozialarbeit liegt in der Beratung der Schülerinnen und Schüler, der Erziehungsberechtigten sowie der Fachpersonen von Seiten der Schule und der Betreuung. Hierfür arbeiten die Schulsozialarbeitenden mit den diversen Akteuren eng zusammen.

Herausforderung Informationsaustausch

Die vielseitigen Aufgaben der Schulsozialarbeit legen nahe, dass zu deren Erfüllung regelmässig interdisziplinär und über Institutionsgrenzen hinweg Informationen ausgetauscht werden müssen. Doch in welcher Art und in welchem Masse ist ein Informationsaustausch möglich, wenn einerseits eine breit gefächerte Zusammenarbeit verlangt wird, andererseits aber ein Vertrauensverhältnis zu den Kindern und Jugendlichen beachtet werden will und Schweigepflichten und Amtsgeheimnis zu berücksichtigen sind? Diese und ähnliche Fragestellungen stell(t)en die Schulsozialarbeitenden vor Herausforderun-

gen und waren Anlass dafür, dass die Datenschutzstelle im Jahr 2014 zu zwei Veranstaltungen eingeladen wurde, welche den Informationsaustausch in der Schulsozialarbeit zum Gegenstand hatten.

Fehlende bereichsspezifische Regeln

Der Grund für die Schwierigkeiten und Verunsicherungen in Bezug auf den Austausch von Informationen in der Schulsozialarbeit war in erster Linie in den fehlenden bereichsspezifischen Rechtsgrundlagen zu sehen. Die damaligen kantonalen Rechtsgrundlagen äusserten sich zwar dahingehend, dass die Gemeinden für ein bedarfsgerechtes Angebot an Schulsozialarbeit sorgen müssen, in Bezug auf den Umgang mit Informationen bestanden jedoch keine Regelungen. Gleich verhielt es sich mit den Rechtsgrundlagen auf städtischer Stufe. Diese regelten einzig die Ausgaben und die organisatorische Zugehörigkeit der Schulsozialarbeit. Da in der Schulsozialarbeit auch sehr sensible Personendaten erhoben, bearbeitet und ausgetauscht werden, hätte sich der Gesetzgeber auch zum Umgang mit diesen Informationen äussern müssen. Dies war zum damaligen Zeitpunkt nicht der Fall und hatte zur Folge, dass für die Beantwortung der Fragen zum Informationsaustausch in der Schulsozialarbeit keine fachspezifischen Rechtsgrundlagen, sondern bloss allgemeine Rechtsprinzipien zur Verfügung standen. Gewisse Rechtsfragen konnten deshalb nicht befriedigend beantwortet und die diesbezüglichen Unsicherheiten und Unklarheiten der Schulsozialarbeitenden nicht in einer sachgerechten und praxistauglichen Weise beseitigt werden.

Die Schulsozialarbeit war ein anschauliches Bespiel dafür, wie wichtig es ist, dass sich der Gesetzgeber auch zum Umgang mit sensiblen Personendaten äussert und passende bereichsspezifische Regeln schafft. Die Schulsozialarbeit der Stadt Zürich verfügte zwar bereits

zum damaligen Zeitpunkt über ein Fachkonzept. Dieses konnte aber fehlende Rechtsgrundlagen nicht ersetzen und hatte nach Ansicht der Datenschutzstelle die Datenbearbeitung und den Informationsaustausch rechtlich zu wenig stringent zum Gegenstand.

Diese Feststellungen veranlassten die Datenschutzstelle im September 2014, die Verantwortlichen der Schulsozialarbeit und die Vorsteher des Schul- und Sportdepartements und des Sozialdepartements auf diese unbefriedigende Situation hinzuweisen und eine entsprechende Klärung des Informationsaustauschs in der Schulsozialarbeit der Stadt Zürich anzuregen. Die in der Folge im Berichtsjahr zwischen Schulsozialarbeit, Departementsrechtsdiensten und Datenschutzstelle intensiv geführte Auseinandersetzung zu Informationsbedarf und Informationsaustausch in der Schulsozialarbeit führte zur Erkenntnis, dass die Ende 2014 lancierte Revision des kantonalen Kinder- und Jugendhilfegesetzes für die Schulsozialarbeit der Stadt Zürich ausreichend sein wird und dass kein Bedarf an allenfalls zusätzlichen städtischen Rechtsgrundlagen besteht. Anzupassen war jedoch das Fachkonzept der Schulsozialarbeit der Stadt Zürich.

Das revidierte Kinder- und Jugendhilfegesetz

Seit Januar 2017 ist das revidierte kantonale Kinder- und Jugendhilfegesetz in Kraft. Dieses sieht im Wesentlichen vor, dass die Schulsozialarbeitenden bei vermuteteter Kindswohlgefährdung die erforderlichen Personendaten bei anderen Verwaltungsangestellten oder Privatpersonen beschaffen und sich mit diesen Stellen und Personen auch entsprechend austauschen können. In allen anderen Belangen, wenn also keine Kindswohlgefährdung zur Diskussion steht, haben die Schulsozialarbeitenden die benötigen Personendaten direkt bei ihren «Klienten», also bei den Kindern und Jugendlichen, zu beschaf-

fen und eine Weitergabe an bzw. ein Austausch mit anderen Stellen und Personen ist nur mit dem Einverständnis der betroffenen Kinder und Jugendlichen zulässig.

Die neuen kantonalen Rechtsgrundlagen im Kinder- und Jugendhilfegesetz regeln die Beschaffung und den Austausch von Personendaten von Kindern, Jugendlichen und deren Familien in einem restriktiven Sinne. Sie setzen für die Informationsbearbeitung Grenzen und geben den Schulsozialarbeitenden insbesondere die Pflicht, ausserhalb von vermuteten Kindwohlgefährdungen in der Regel keine Daten, die sich auf bestimmte Kinder oder Jugendliche beziehen, bekannt zu geben. Diese Vorgaben des kantonalen Gesetzgebers werden nicht nur die Schulsozialarbeitenden zu beachten haben, sondern ebenso auch diejenigen Stellen, die regelmässig mit Schulsozialarbeitenden in Kontakt stehen, insbesondere diejenigen aus dem Schulbereich.

Die neuen Rechtsgrundlagen im kantonalen Kinder- und Jugendhilfegesetz beziehen sich nur auf Personendaten. Informationen, die sich nicht auf einzelne Personen beziehen wie bspw. fachliche Auskünfte oder solche, die ganze Klassen betreffen, unterliegen nicht diesen Einschränkungen. All diejenigen Tätigkeiten der Schulsozialarbeitenden, die keine Bearbeitung von Personedaten im Sinne der Datenschutzgesetzgebung beinhalten, werden deshalb von diesen Rechtsgrundlagen nicht tangiert sein.


GROSSSTADTRAUSCH/NATURIDYLL

C) Forschung und Statistik

In ihren Jahresberichten macht die Datenschutzstelle regelmässig auf Bedeutung und Komplexität von Datenbearbeitungen zu sogenannt nicht personenbezogenen Zwecken – also beispielsweise für Forschung, Statistik oder Planung – aufmerksam. Politik, Wirtschaft, Öffentlichkeit und Medien verlangen für ihre Beurteilungen und Entscheidungen immer mehr nach Umfragen, Auswertungen und Kennzahlen. Die Verwaltung ist dabei mit ihren zahlreichen und zuverlässigen Informationsbeständen eine gefragte Datenlieferantin.

Die Voraussetzungen, die die Datenschutzgesetzgebung für solche Datenbekanntgaben zu Forschungs- oder Statistikzwecken verlangt, scheinen klar und einfach zu sein: Die Daten müssen rechtzeitig anonymisiert werden und Rückschlüsse auf betroffene Personen dürfen nicht möglich sein. Auch die rechtlichen Konsequenzen, die sich daraus ergeben, scheinen klar und einfach zu sein: Anonymisierte Daten sind keine Personendaten mehr und fallen deshalb nicht (mehr) unter die Datenschutzgesetzgebung. So weit so gut. Weniger klar und einfach beantworten lässt sich aber regelmässig die Frage, wie diese gesetzlichen Vorgaben erreicht werden können. Im Zeitalter zunehmender Digitalisierung und Big Data und der sich daraus ergebenden Analyse- und Verknüpfungsmöglichkeiten erweist sich insbesondere die Anonymisierung von Personendaten als ein immer schwierigeres Unterfangen. Eine entsprechend sorgfältige datenschutzrechtliche Prüfung ist deshalb auch bei Bearbeitungen und Bekanntgaben von Verwaltungsdaten zu Forschungs-, Statistik- oder Planungszwecken wichtig. Die nachfolgenden drei Beispiele aus dem Berichtsjahr verdeutlichen dies.

1. Nationales Herzchirurgie-register

Medizinische Register gewinnen in der Schweiz immer mehr an Bedeutung. Traditionell werden medizinische Register in der epidemiologischen Forschung eingesetzt. Das Anwendungsspektrum medizinischer Register hat sich in den letzten Jahren jedoch stark ausgeweitet. Heute liefern medizinische Register auch wichtige Grundlagendaten für die klinische Forschung, für die Versorgungs- und Ursachenforschung, für die Qualitätssicherung sowie für die Gesundheitspolitik. Gemäss der Online-Plattform «Medizinische Register Schweiz» der Verbindung der Schweizerischen Ärztinnen und Ärzte FMH werden schweizweit über 70 medizinische Register geführt. Die Verantwortung für diese Register obliegt in der Regel den einzelnen medizinischen Fachgesellschaften. Technisch betrieben werden die Register vorwiegend von spezialisierten privaten Unternehmen.

Fehlende spezifische Regelungen

Obwohl in den schweizweit geführten medizinischen Registern sensible Patientendaten im grossen Stil bearbeitet werden, fehlen bis heute weitgehend klare und detaillierte gesetzliche Regelungen für die Führung solcher Register. Eine löbliche Ausnahme ist das nationale Krebsregister, für welches auf Bundesebene ein Gesetz mit entsprechenden datenschutzrechtlichen Rahmenbedingungen geschaffen wurde. Die meisten anderen Register stützen sich auf die generellen Bestimmungen des Humanforschungsgesetzes sowie im Bereich der Qualitätssicherung auf die betreffenden Bestimmungen der obligatorischen Krankenversicherung. Die im Berichtsjahr von di-

versen Akteuren im Gesundheitsbereich gemeinsam verabschiedeten «Empfehlungen zum Aufbau und Betrieb von gesundheitsbezogenen Registern» fangen immerhin inhaltlich die fehlenden gesetzlichen Regelungen etwas auf. Die Empfehlungen enthalten umfassende und zum Teil detaillierte datenschutzrelevante Vorgaben, insbesondere betreffend Verantwortlichkeiten, Zweckbindung der Register, Datenerhebung und -aufbewahrung, Einsichts- und Zugriffsrechte, Datenhoheit, Verwendung der Daten durch Dritte sowie Informationssicherheit. Aufgrund der hohen Sensibilität medizinischer Register wäre es aus Datenschutzoptik zu begrüssen, wenn der Umgang mit solchen Registern durch den Gesetzgeber verbindlich geregelt würde.

Herzchirurgieregister

Im Berichtsjahr hatte sich die Datenschutzstelle vertieft mit dem Nationalen Herzchirurgieregister auseinanderzusetzen. Anlass hierfür war die Anbindung des Stadtspitals Triemli an dieses Register, welches in den letzten Jahren unter der Verantwortung der Schweizerischen Gesellschaft für Herz- und Thorakale Gefässchirurgie (SGHC) primär zu Qualitätssicherungszwecken aufgebaut wurde. Ob Bypass-, Herzklappen- oder Hauptschlagader-Operationen, alle chirurgischen Eingriffe am Herzen, allfällige Komplikationen sowie die Sterberaten werden in das Herzchirurgieregister eingetragen. Im Herzchirurgieregister selber sind keine Personendaten erfasst. Zugriff auf das Herzchirurgieregister haben die verschiedenen Kliniken im Bereich der Herzchirurgie. Diese können aber lediglich ihre eigenen Daten analysieren und die Resultate mit dem Gesamtkollektiv der in der Schweiz erfassten Daten vergleichen. Insofern ist das Herzchirurgieregister aus Datenschutzoptik als nicht weiter problematisch zu bezeichnen.

Einbindung in ein integrales System

Betrieben wird das Nationale Herzchirurgieregister auf einem integralen medizinischen Datenbearbeitungssystem der Schweizerischen Post. Das System dient den medizinischen Leistungserbringern neben der Führung weiterer medizinischer Register zum Teil auch als klinisches Patientendokumentationssystem sowie als Zuweisungs- und Überweisungsportal. Dabei sind die medizinischen Register und die weiteren medizinischen Dokumentationen nicht als abgeschottete Insellösungen konzipiert. Register und Patientendokumentationen sind mit einem in das Gesamtsystem integrierten Modul verknüpft, in welchem verschiedene persönliche Stammdaten eines Patienten oder einer Patientin wie Namen, Vornamen, Geburtsdatum, AHV-Nummer erfasst werden. Zugang zu diesen Patientenstammdaten haben – im Gegensatz zu den medizinischen Daten in den Registern – alle Nutzerinnen und Nutzer des Systems.

Wie bei den meisten medizinischen Registern, welche Dritten nur anonymisierte Abfragen erlauben, müssen auch im Herzchirurgieregister die Chirurginnen und Chirurgen ihre eigenen Patientinnen und Patienten (re)identifizieren können. Dies wird im System der Post durch die Verknüpfung der medizinischen Registerdaten mit den Patientenstammdaten ermöglicht. Eine solche Verknüpfung führt allerdings automatisch auch zur Verknüpfung der verschiedenen Register und Patientendokumentationen. Das System hat damit das technische Potential für umfassende, patientenbezogene Datenauswertungen. Damit dies nicht unberechtigterweise geschieht, verfügt das System über eine entsprechende Berechtigungssteuerung. So bestimmen einerseits die Fachgesellschaften über den Zugang zu den anonymisierten Daten in den medizinischen Registern und andererseits liegt es in der Hand der behandelnden Ärztinnen und Ärzte, Dritten die Berechtigungen auf Zugang zu Daten ihrer Patientinnen

und Patienten zu gewähren. Trotz dieser Berechtigungssteuerung, welche sich am ärztlichen Berufsgeheimnis orientiert, ist eine solche Verknüpfung von verschiedenen medizinischen Registern und Patientendokumentationen in einem zentralen Datensystem mit entsprechenden Risiken verbunden. Das für diese Datenplattform verfasste Datenschutzkonzept wurde vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geprüft. In einer summarischen Beurteilung hat dieser festgehalten, dass das Datenschutzkonzept geeignet erscheine, um Datenschutz- und Datensicherheit zu gewährleisten. Zum Herzchirurgieregister selber hat der EDÖB keine Aussage gemacht.

Lösung für das Stadtspital Triemli

Aufgrund der Abklärungen der Datenschutzstelle bei der Klinikleitung des Stadtspitals Triemli konnte festgestellt werden, dass für die Zwecke des Herzchirurgieregisters keine Notwendigkeit für eine Verknüpfungsmöglichkeit dieses Registers mit anderen medizinischen Registern oder spitalfremden Patientendokumentationen besteht. Die Datenschutzstelle hat daher darauf hingewirkt, dass die Anbindung des Stadtspitals Triemli an das nationale Herzchirurgieregister ohne eine solche Verknüpfungsmöglichkeit umgesetzt wird. Dies kann erreicht werden, indem im Stammdatenmodul des Systems lediglich die spitalinterne Patienten- und Fallnummer (als sogenannte Pseudonyme) eines Patienten erfasst werden. Mit diesen Angaben können die Herzchirurgen des Stadtspitals Triemli ihre Patientinnen und Patienten über das spitalinterne Patienteninformationssystem identifizieren. Die Herzchirurgiepatientinnen und – patienten des Stadtspitals Triemli können damit sicher sein, dass ihre freiwillig offenbarten Daten nicht mit Daten aus anderen medizinischen Registern verknüpft werden können.

Ausblick

Bereits heute ist absehbar, dass die Forschung, die Gesundheitspolitik, die Kranken- und Unfallversicherer, aber auch die Leistungserbringer selber vermehrt nach Register übergreifenden Auswertungen und Kennzahlen verlangen werden. Dies setzt die Verknüpfbarkeit medizinischer Register voraus, was nur über entsprechende Patientendatenstammdaten bzw. über eindeutige, institutionsübergreifende Identifikatoren möglich sein wird. Aufgrund der hohen Sensibilität solcher Verknüpfungen werden entsprechende Standardisierungen und verbindliche Regelungen auf nationaler Ebene unentbehrlich sein. Als Beispiel hierfür sei das neue Krebsregistrierungsgesetz erwähnt, welches eine institutionsübergreifende Verknüpfung von Patientendaten über einen eindeutigen Identifikator vorsieht, die Erzeugung dieses Identifikators allerdings einer von der Krebsregistrierungsstelle unabhängigen Pseudonymisierungsstelle überträgt.

2. Städtische Mitarbeitendenbefragung

Die Befragung von Mitarbeiterinnen und Mitarbeitern zu Themen wie Arbeit oder Gesundheit spielt seit längerem in der Privatwirtschaft und zunehmend auch in der öffentlichen Verwaltung eine immer grössere Rolle. Ende Februar 2017 startete die Stadt Zürich unter dem Titel «Arbeit und Gesundheit» ihre mittlerweile dritte stadtweite Mitarbeitendenbefragung. Rund 28 000 Mitarbeitende der Stadtverwaltung und der städtischen Schulen wurden gebeten, an dieser Online-Umfrage teilzunehmen und unter anderem sensible Fragen zu ihrer physischen und psychischen Gesundheit (beispielsweise hinsichtlich Rückenschmerzen, Einschlaf- und Durchschlafstörungen, Herzstolpern), zu ihrer Leistungsfähigkeit und Motivation im Arbeitsverhältnis sowie zu allfälligen sexuellen Belästigungen am Arbeitsplatz zu beantworten.

Mitarbeitendenumfragen sind nur sinnvoll, wenn aus den Befragungsdaten aussagekräftige Auswertungen möglich sind und wenn bei Bedarf konkrete Massnahmen daraus abgeleitet werden können. Dies setzt erst einmal voraus, dass eine genügend grosse Anzahl der Mitarbeitenden an einer solchen Befragung teilnimmt. Damit dies erreicht werden kann, müssen die Mitarbeitenden in einen korrekten Umgang mit ihren persönlichen Angaben vertrauen können. Sie müssen also sicher sein, dass ihre Antworten keinerlei Konsequenzen in Bezug auf ihr Arbeitsverhältnis haben werden. Eine solche Sicherheit kann im Wesentlichen nur dann erreicht werden, wenn erstens die Arbeitgeberin keinen Zugang zu den Befragungsdaten hat, zweitens nur Auswertungen vorgenommen werden, die keinerlei Rückschlüsse auf die einzelnen Mitarbeitenden erlauben und drittens die Mitarbeitenden transparent informiert sind. Auf diese Anforderungen legte die

Datenschutzstelle – wie nachfolgend ausgeführt – im Rahmen ihrer Beratungs- und Aufsichtstätigkeit besonderes Augenmerk.

Befragung und Auswertung durch verwaltungsexternes Unternehmen

Die Auslagerung von Datenbearbeitungen ist gestützt auf das Datenschutzrecht zwar zulässig, wird aber in der Regel eher als datenschutzrechtliches Risiko angesehen (bespielsweise bei der Speicherung von Verwaltungsdaten in der Cloud). Gerade umgekehrt verhält es sich bei sensiblen Mitarbeitendenbefragungen: Bei solchen Befragungen zeigt sich, dass wichtige datenschutzrechtliche Anforderungen, insbesondere die Gewährleistung der Vertraulichkeit, nur mit einer konsequenten Auslagerung der Datenbearbeitung an ein externes Unternehmen zu bewerkstelligen sind. Damit sichergestellt werden konnte, dass die Stadt Zürich als Arbeitgeberin keinen Zugang zu den Befragungsdaten haben wird, wurden sämtliche Erhebungen und Auswertungen der städtischen Mitarbeitendenbefragung an ein externes Unternehmen übertragen. Die Prozesse der Datenbearbeitungen und die damit verbundenen Zuständigkeiten und Verantwortlichkeiten wurden zwischen der Stadt Zürich als Auftraggeberin und dem externen Unternehmen als Auftragnehmerin in einem Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) verbindlich geregelt. An diese Vorgaben sind insbesondere auch die Dienstchefinnen und Dienstchefs gebunden, welche beim externen Unternehmen zusätzliche Spezialauswertungen über ihre Dienstabteilungen in Auftrag geben können.

Anonymisierte Auswertungsergebnisse

Die Stadt Zürich als Arbeitgeberin hat ein nachvollziehbares Interesse an möglichst detaillierten und damit aussagkräftigen Auswertungen. Je genauer die Auswertungen allerdings Bezug auf die einzelnen Organisationseinheiten nehmen, umso grösser ist das Risiko, dass – beispielsweise bei entsprechendem Insiderwissen – Rückschlüsse auf einzelne Mitarbeitende möglich werden. Es gilt also die richtige Balance zwischen dem Bedürfnis der Arbeitgeberin nach möglichst aufschlussreichen Detailauswertungen und der Gewährleistung der Anonymität der einzelnen Mitarbeitenden zu finden. Bei der städtischen Mitarbeitendenbefragung zusätzlich zu berücksichtigen war das im IDG statuierte Öffentlichkeitsprinzip, wonach interessierten Personen oder Institutionen grundsätzlich ein Anspruch auf Zugang zu den anonymisierten Auswertungsergebnissen zusteht. Insbesondere Personalverbände waren an den Ergebnissen der letzten Mitarbeitendenbefragungen interessiert und verlangten Zugang zu den entsprechenden Auswertungen. Diese Zugänglichkeit der Auswertungsergebnisse erhöht damit die Anforderungen an die Datenanonymisierung zusätzlich. Gestützt auf diese Ausgangssituation wurden bei der städtischen Mitarbeitendenbefragung im ISDS-Konzept die zulässigen Auswertungen auf den Stufen Stadt, Departement und Dienstabteilungen bestimmt und verbindliche und klar definierte Anforderungen an die Datenanonymisierung festgelegt. Damit soll sichergestellt werden, dass das beauftragte Unternehmen nur solche Auswertungen vornimmt und der Stadt Zürich als Arbeitgeberin bekannt gibt, welche keine Rückschlüsse auf die Mitarbeitenden erlauben.

Schaffung von Transparenz

Die Stadtpräsidentin und der Vorsteher des Finanzdepartements haben zum Start der Mitarbeitendenbefragungen alle städtischen Angestellten über den Zweck der Befragung, den Beizug des externen Unternehmens und insbesondere über die Gewährleistung der Datenanonymisierung informiert. Die Bearbeitungs- und Auswertungsdetails wurden auch im «Konzept zur Vorbereitung und Durchführung der Mitarbeitendenbefragung 2017» festgehalten, welches zusammen mit dem dazu gehörigen Stadtratsbeschluss im Internet veröffentlicht wurde. Zudem wurden in der eigens für die Durchführung der städtischen Mitarbeitendenbefragung erstellten Website die Mitarbeiterinnen und Mitarbeiter über die wesentlichen Rahmenbedingungen der Befragung informiert. Mit all diesen Kommunikationsmassnahmen hat die Stadt den Umgang mit den Befragungsdaten von Anfang an offen gelegt und damit gegenüber ihren Mitarbeiterinnen und Mitarbeiter die notwendige Transparenz geschaffen.

3. Veröffentlichung von Umfragedaten auf OGD-Portal

Vor rund sieben Jahren hat die Stadt Zürich schweizweit das erste Open Government Data-Portal (OGD-Portal) gestartet. Ziel dieses Portals ist der offene Zugang zu Behördendaten und deren freie Verwendung. Interessierte Kreise sind eingeladen, auf Basis dieser Daten innovative Informationsdienstleistungen zu entwickeln. Bis anhin wurden vor allem zahlreiche Geoinformationen wie etwa der Stadtplan, das Strassennamenverzeichnis, aber auch statistische Daten der Gebäude- und Wohnungsstatistik oder die Resultate verschiedener Abstimmungen der Öffentlichkeit in maschinenlesbarer Form zugänglich gemacht. Die verfügbaren Daten auf dem OGD-Portal sollen laufend erweitert werden.

Das OGD-Portal stiess von Beginn an auf positive Resonanz. Auf der Basis frei verfügbarer Behördendaten sind in den letzten Jahren auf private Initiative hin zahlreiche Anwendungen entstanden: So beispielsweise die App «Badi Zürich – Freibäder», mit der auf einen Blick alle Standorte von städtischen Freibädern samt Informationen zu Öffnungszeiten und aktuell gemessenen Wassertemperaturen angezeigt werden können, die App «Veloverleih», mit der alle Standorte der Verleihstationen von «Züri rollt» mit den öffentlich zugänglichen Velopumpstationen sowie den aktuell verfügbaren Leihfahrräder in Echtzeit abgerufen werden können oder etwa die App «ParkenDD», mit der freie Parkhausplätze in Echtzeit angezeigt und auf einer Karte dargestellt werden können.

Rechtliche Rahmenbedingungen

Rechtlich stützt sich das OGD-Portal auf den Öffentlichkeitsgrundsatz ab, der in der Kantonsverfassung und im Gesetz über die Information und den Datenschutz verankert ist und die Verwaltung verpflichtet, von sich aus über ihre Tätigkeiten von allgemeinem Interesse zu informieren. Der Stadtrat hat die rechtlichen Rahmenbedingungen solcher Veröffentlichungen und die damit zusammenhängenden Verantwortlichkeiten in einer OGD-Policy sowie in OGD-Richtlinien detailliert geregelt. Die Datenschutzstelle hat an der damaligen Ausarbeitung dieser Regelungen massgeblich mitgewirkt.

Keine Veröffentlichung von Personendaten

In der OGD-Policy werden Daten, welche durch höhere rechtliche Interessen wie insbesondere Amtsgeheimnis, Datenschutz, übergeordnete öffentliche Interessen oder Urheberrecht geschützt sind, von der Veröffentlichung ausgenommen. Personendaten, d. h. Daten, die einen Personenbezug aufweisen können und dadurch in den Geltungsbereich der Datenschutzgesetzgebung fallen, dürfen auf dem OGD-Portal grundsätzlich nicht zur Verfügung gestellt werden. Will eine Verwaltungsstelle einen Informationsbestand, der Personendaten enthält, über das OGD-Portal veröffentlichen, kann sie dies erst tun, wenn sie vorgängig den Personenbezug eliminiert hat. Eine Veröffentlichung von Daten über das OGD-Portal setzt also voraus, dass diese vorgängig anonymisiert wurden.

Die Anonymisierung von Personendaten ist in der Praxis oft ein schwieriges Unterfangen, welches ohne Fachkenntnisse und vertiefte Abklärungen nicht bewerkstelligt werden kann. Ein spezielles Gewicht erhält das Thema der Datenanonymisierung bei OGD, da

die Daten der Öffentlichkeit in maschinenlesbarer Form zur freien Verfügung gestellt werden. Interessierte Kreise wie beispielsweise App-Entwickler können mit den Daten grundsätzlich tun, was sie wollen. Die Datensätze können insbesondere untereinander oder mit anderen verfügbaren Datensätzen nach Belieben verknüpft werden. Dadurch besteht ein latentes Risiko, dass durch die Verknüpfung der an sich anonymisierten Datensätze die Anonymisierung wieder aufgehoben wird. Bei Veröffentlichungen auf dem OGD-Portal ist daher der Datenanonymisierung erhöhte Aufmerksamkeit zu schenken. Im Berichtsjahr hatte sich die Datenschutzstelle bei einem Vorhaben der Stadtentwicklung vertieft mit dieser Thematik auseinanderzusetzen.

Daten der Bevölkerungsbefragung

Ergebnisse aus Bevölkerungsbefragungen werden in der Regel in Form von Berichten mit statistischen Auswertungen publiziert. Inhalt der Publikationen und Interpretation der erhobenen Daten werden durch die Verfasser bzw. die Auftraggeber der Befragungen bestimmt. Bei den Bevölkerungsbefragungen der Stadt Zürich waren dies bespielsweise Themen wie «Dynamik, bauliche Veränderungen und Dichte» (mit Aussagen wie «9% der Befragten finden, dass die Stadt Zürich sehr dicht bebaut ist»), oder «Verkehr» (mit Aussagen wie «96% fühlen sich wohl und komfortabel zu Fuss unterwegs»). Ergebnisse oder Resultate aus Befragungen dürfen dabei nur anonymisiert veröffentlicht werden. Hierfür müssen die erhobenen Daten aggregiert, d. h. soweit zusammengefasst werden, dass keine Rückschlüsse auf einzelne Personen möglich sind.

Mit der jüngsten Bevölkerungsbefragung aus dem Jahre 2015 wollte die Stadt Zürich nun neue Wege beschreiten und erstmals nicht bloss Auswertungen oder Berichte publizieren, sondern über das

OGD-Portal auch einen Teil der erhobenen Daten veröffentlichen (sogenannte Befragungs- oder Rohdaten). Damit sollte erreicht werden, dass Befragungsdaten, die die Basis für anschliessende Auswertungen darstellen, nicht wie bis anhin nur für die «offiziellen» Berichte, sondern auch für weitere (private) Auswertungen oder anderweitige Verwendungen zur Verfügung stehen.

Wie bei der herkömmlichen Veröffentlichung in Berichtsform war selbstverständlich auch bei der OGD-Publikation zu gewährleisten, dass die Daten keine Rückschlüsse auf befragte Personen ermöglichen. Da die Befragungsdaten der Bevölkerungsbefragung 2015 – wie bei jeder derartigen Befragung üblich – nicht nur die eigentlichen Antworten auf die in der Umfrage gestellten Fragen enthalten, sondern ebenso eine Vielzahl demographischer Angaben der Befragten wie beispielsweise Alter, Geschlecht, Wohnort, Nationalität, Beruf, Aufenthaltsstatus oder Haushaltseinkommen, erwies sich eine entsprechende Anonymisierung als schwieriges Unterfangen. Je mehr demographische Angaben bei einer Befragung erhoben werden, desto genauer und spezifischer lassen sich zwar Aussagen oder Erkenntnisse herleiten und zuordnen, desto grösser ist aber gleichzeitig auch die Möglichkeit, Personen, die an einer Befragung teilgenommen haben, zu eruieren und Aussagen aus der Befragung diesen Personen zuzuordnen. Aufgrund dieser Rückschlussmöglichkeiten werden solche Befragungs- oder Rohdaten denn auch üblicherweise nicht zugänglich gemacht und gelöscht, sobald eine Umfrage oder Studie abgeschlossen und ausgewertet ist.

Auch die Befragungsdaten der Bevölkerungsbefragung 2015 konnte nur durch entsprechende Datenaggregation anonymisiert werden. Im Resultat bedeutete dies, dass die meisten demographischen Angaben zu (meist pauschalen) Kategorien zusammengefasst oder ganz gelöscht werden mussten. Die Publikation von Datensätzen aus der

Bevölkerungsbefragung 2015 auf dem OGD-Portal erlaubte zwar, dass weitergehende Informationen als bei den früheren Bevölkerungsbefragungen zur Verfügung gestellt werden konnten. Gleichzeitig zeigte sich aber auch, dass Rohdaten aus Erhebungen und Umfragen nur in beschränktem Masse «OGD-tauglich» sind, da die aus Datenschutzgründen verlangte Aggregation der demographischen Angaben stets dazu führen wird, dass nur ein Bruchteil der ursprünglichen Befragungsdaten als unbeschränkt weiterverwendbar zugänglich gemacht werden können.

Eine stichprobenweise Überprüfung der aufbereiteten Datensätze durch Statistik Stadt Zürich bestätigte die korrekte Anonymisierung, so dass festgestellt werden konnte, dass die datenschutzrechtlichen Anforderungen gemäss IDG und OGD-Policy erfüllt sind und die aggregierten Befragungsdaten auf dem OGD-Portal veröffentlicht werden konnten. Wie bei allen Veröffentlichungen von Informationsbeständen auf einem OGD-Portal konnte auch bei den Befragungsdaten eine Prüfung nur nach aktuellem Kenntnisstand erfolgen. Eine absolute Gewähr dafür, dass auch bei Einsatz zukünftiger Technologien jeglicher Personenbezug unter allen Umständen ausgeschlossen bleibt, kann nicht erwartet oder abgegeben werden.


FreiRaum
Primavera

D) Informationssicherheit

Wie steht es um die Sicherheit der Daten und Informationen in der Stadtverwaltung?

NACHGEFRAGT bei Anja Harder. Sie war bis Januar 2017 Leiterin der Fachstelle Informationssicherheit bei der OIZ der Stadt Zürich. Seither ist sie Chief IT Security Officer der Informatikdienste der ETH Zürich. Die Sicherheit der Daten und Informationen ist eine der zentralen Forderungen aus der Datenschutzgesetzgebung. Für ihre diesbezüglichen Aufgaben arbeiten die Fachstelle Informationssicherheit der OIZ und die Datenschutzstelle der Stadt Zürich regelmässig eng zusammen.

Sie waren während 5½ Jahren oberste Verantwortliche für Informationssicherheit der Stadtverwaltung. Lässt einen eine solche Verantwortung noch gut schlafen?

Das Bewusstsein, in einer starken und kompetenten Organisation zu arbeiten, die ihre Hausaufgaben bezüglich Sicherheitsvorkehrungen macht, steigert die Schlafqualität sehr.

Fast täglich berichten die Medien über Angriffe aus dem Cyberspace, in letzter Zeit vor allem über Datenklau und Erpressungsversuche. In welchem Masse ist auch die Stadtverwaltung von solchen externen Angriffen betroffen?

Natürlich ist auch die Stadtverwaltung solchen Angriffen ausgesetzt. Ein beliebter Angriffsvektor ist nach wie vor E-Mail. Mittels geschickt angefertigten «Phishing Mails» sollen Empfänger auf infizierte Websites gelockt werden. Klicken sie auf die Links in diesen Mails,

werden PC und Benutzerkonto mit Schadprogrammen infiziert. In diesem Zusammenhang ist es z. B. zu kleinen Vorfällen von Erpressungsversuchen mittels sogenannter Ransomeware gekommen. Mit Ransomeware infizierte Computer verschlüsseln die Daten im Zugriff des betroffenen Benutzenden. Die Angreifer verlangen dann eine Lösegeldzahlung für die Entschlüsselung. Zu solchen Zahlungen ist es in der Stadtverwaltung nicht gekommen. Die Angriffe konnten jeweils schnell gestoppt und verschlüsselte Datenbestände aus Backups wiederhergestellt werden.

Welches sind die Gegenmassnahmen der Stadtverwaltung? Wie erfolgreich sind sie?

Die Stadtverwaltung setzt eine ganze Reihe von Gegenmassnahmen in unterschiedlichen Bereichen der ICT-Infrastruktur ein, die aus naheliegenden Gründen nicht detailliert geschildert werden können. Natürlich werden Filter eingesetzt, die möglichst viele der unerwünschten Mails abfangen, bevor sie in die Mailboxen der Benutzenden gelangen. Eindrücklich ist nur schon die Anzahl der E-Mails, die durchschnittlich im SPAM-Filter hängenbleiben: Pro Monat werden rund 35 Millionen E-Mails von extern an die Stadtverwaltung zugestellt. Davon werden fast 96% ausgefiltert. Doch wie immer: es gibt keine absolute Sicherheit. Es kommt immer wieder vor, dass es Phishing Mails bis in die Mailboxen der Benutzenden schaffen. Es sind Massnahmen implementiert, um auch diese Fälle möglichst schnell entdecken und behandeln zu können. Diese Mechanismen sind so erfolgreich, dass die Geschäftsprozesse der Stadtverwaltung bisher nicht aufgrund von Ransomeware oder anderen Attacken beeinträchtigt worden sind.

Bei der Informationssicherheit gibt es ja nicht nur die Angriffe von aussen. Wie kann sich eine Verwaltung oder ein Unternehmen gegenüber internen Angriffen schützen?

Viele der eingesetzten Schutzmassnahmen wirken unabhängig davon, ob der Angriff von extern oder intern gestartet wird. Das Sicherheitsdispositiv ist längst nicht mehr nur darauf fokussiert, Angriffe an den Aussengrenzen des Netzes – etwa an einer Firewall – abzuwehren. Das wäre in Zeiten von «Bring your Own Device», «Cloud Computing» und «Internet of Things» nicht mehr ausreichend. Abgesehen vom Schutz an den Aussengrenzen des städtischen ICT-Netzes ist ein ganzes Bündel an Schutzmassnahmen implementiert, dass darauf zielt, unautorisierte Personen und Systeme fernzuhalten, bekannte Schadprogramme aufzuspüren und verdächtige Aktivitäten zu erkennen.

Moderne Technologie soll nicht nur zu immer mehr Digitalisierung führen, sie soll auch die Informationssicherheit laufend verbessern. Welche Technologien werden uns in Zukunft grössere Sicherheit bringen?

Es gibt einige vielversprechende Lösungen und Ansätze. Ein wichtiges Thema dabei ist die Benutzungsfreundlichkeit: Sicherheitslösungen werden häufig immer noch als umständlich, schwierig und störend wahrgenommen. Die Zukunft wird Lösungen bringen, die vertrauenswürdige und einfach handhabbare sichere Anmeldungen an Systeme bieten. Eine solche Lösung sollte möglichst weitreichend einsetzbar sein, so dass Benutzende zukünftig nur noch mit einer möglichst kleinen Anzahl von Authentisierungsmitteln jonglieren müssen. Ebenfalls in den Bereich der Benutzungsfreundlichkeit fallen die Themen «E-Mail-Signatur und –E2E-Verschlüsselung». Hier sind niederschwellig einsetzbare Lösungen gefragt, die auch organisationsübergreifende E-Mail-Kommunikation absichern. Signierter und verschlüsselter E-Mail-Verkehr wird hoffentlich bald im geschäftlichen wie im privaten Umfeld zur Selbstverständlichkeit. Der konsequente Einsatz von E-Mail-Signaturen kann übrigens auch dazu beitragen, die Erfolgsraten von Phishing-Angriffen zu senken.

Ein anderes grosses Thema ist die Erkennung von erfolgreichen Angriffen in komplexen ICT-Umgebungen. In diesem Kontext werden Technologien, die es ermöglichen, Angriffe auf Endgeräten und im Netzwerk aufzuspüren und zu bewerten, vermehrt an Bedeutung gewinnen. Dafür werden Expertensysteme eingesetzt werden, die mit Mechanismen der Künstlichen Intelligenz Analysen in nahezu Echtzeit durchführen. Das ist wichtig, weil trotz aller präventiver Massnahmen nicht ausgeschlossen werden kann, dass Firmen- oder Verwaltungsnetze kompromittiert sind. Es gilt also, erfolgreiche Angriffe schnellstmöglich aufzuspüren und zu stoppen.

Eine weitere wichtige Baustelle ist der präventive Schutz vor Schadprogrammen. Es geht darum zu verhindern, dass Schadprogramme überhaupt auf Systeme gelangen können. Hier gibt es bereits innovative Lösungen, die über den klassischen Ansatz von sogenannten «Virenscannern» hinausgehen und mittels unterschiedlicher Mechanismen nicht nur die anhand ihrer Signaturen bekannten Computerviren, sondern auch noch unbekannte Schadprogramme identifizieren können.

Der Stadtrat hat 2014 das neue Handbuch für Informationssicherheit erlassen. Wie wichtig sind solche Regulative für die Gewährleistung von Informationssicherheit? Welche Bedeutung kommt internationalen Standards zu?

In einer komplexen ICT-Umgebung wie derjenigen der Stadt Zürich ist es unumgänglich, Leitplanken festzulegen, an die sich alle Teilnehmenden halten müssen. Dies vor allem, damit zu schwach gesicherte Systeme nicht andere Plattformen gefährden. Die Regelungen im Handbuch Informationssicherheit legen die personellen, organisatorischen und technischen Anforderungen an die Informationssicherheit für alle beteiligten Menschen, Systeme und Daten fest. Es

wäre deutlich ineffizienter, solche Regelungen für jede Plattform oder Systemumgebung einzeln zu erarbeiten und zu vernehmlassen.

Internationale Standards – im Fall der Stadt Zürich ISO/IEC 27001 – haben den Vorteil, von grosser internationaler Expertise zu profitieren. Sie decken quasi alle Themenbereiche ihres jeweiligen Fachgebiets ab und werden laufend aktuellen Entwicklungen angepasst. Anwender solcher Standards profitieren, indem sie nicht jeder für sich «das Rad neu erfinden» müssen. Darüber hinaus erleichtern solche Standards natürlich auch die Kommunikation in organisationsübergreifenden Arbeitsgruppen erheblich.

Die Fachstelle Informationssicherheit gehört zur OIZ, untersteht also der Weisungsbefugnis von OIZ und Finanzdirektion. Müsste eine Fachstelle für Informationssicherheit nicht unabhängiger sein? Kann sie so ihre Prüfungsaufgabe überhaupt wahrnehmen?

Zu den Hauptaufgaben der Fachstelle gehören die Steuerung der Informationssicherheit, die Beratung von Projekten und das Durchführen von Sensibilisierungsmassnahmen. Für diese Tätigkeiten ist die Einbindung in die OIZ und somit die Nähe zu vielen laufenden strategischen ICT-Vorhaben ein Vorteil. Das Wahrnehmen des Prüfungsauftrags war bisher unproblematisch. Tatsächlich lässt die Fachstelle Informationssicherheit jährlich ca. 15 Audits durchführen. Sollte dennoch einmal ein Interessenskonflikt eintreten, kann die Leitung der Fachstelle Informationssicherheit über die IT-Delegation des Stadtrats oder die Datenschutzstelle eskalieren.

Ohne Rücksicht auf das Machbare: Was würde zur Informationssicherheit in der Stadtverwaltung am meisten beitragen?

Hier sind sicher an erster Stelle die laufenden Vorhaben zur «Cyber Defense» zu nennen, vor allem der Aufbau des «Security Operation Centers» (SOC) und die Ausrüstung des SOCs mit den effektiven Werkzeugen. Darüberhinaus wären benutzerfreundliche Lösungen für die zuvor erwähnten Problematiken zur sicheren Authentisierung und Email-Sicherheit wertvoll. Zusätzlich zu guten technischen Lösungen braucht es für die Benutzenden noch drei weitere Massnahmen: AWARENESS, SENSIBILISIERUNG und AWARENESS.

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

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

Patrizia Zbinden, lic. iur.
juristische Mitarbeiterin (80%)

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

Monika Niederberger
Sekretariat (20%)

Quelle Fotos:
Marcel Studer

Gestaltung:
Stadt Zürich, PrintShop

Stadt Zürich
Datenschutzbeauftragter
Beckenhofstrasse 59
8006 Zürich
Tel. 044 412 16 00
datenschutz@zuerich.ch
www.stadt-zuerich.ch/datenschutz