dsb

datenschutzbeauftragter
kanton zürich

Tätigkeitsbericht 2018

Der Beauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht (§ 39 IDG). Der vorliegende Tätigkeitsbericht deckt den Zeitraum vom 1. Januar 2018 bis und mit 31. Dezember 2018 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Mit der Gliederung des Tätigkeitsberichts 2018 macht der Datenschutzbeauftragte auf die besonderen Herausforderungen der Digitalisierung für den Datenschutz und die Sicherheit der Daten aufmerksam. Einerseits nimmt die Datenmenge exponentiell zu, wozu auch sehr viele sensitive Daten gehören. Gleichzeitig verlangen neue Anwendungen nach Agilität dieser Daten, wobei die komplexen Datenbearbeitungen ein zunehmendes Risiko für die persönliche Freiheit darstellen. Dabei ist daran zu denken, dass der Datenschutz nichts anderes ist als der Schutz der Freiheitsrechte der Bürgerinnen und Bürger.

Zürich, im April 2019

Der Datenschutzbeauftragte des Kantons Zürich

Dr. Bruno Baeriswyl

Datenschutz-beauftragter des Kantons Zürich

– Der Datenschutzbeauftragte (DSB) beaufsichtigt die Datenbearbeitungen der kantonalen Verwaltung, der Gemeinden und der übrigen Behörden und öffentlichen Einrichtungen im Kanton, um die Privatheit der Bürgerinnen und Bürger sicherzustellen.

– Er berät die öffentlichen Organe, beurteilt die datenschutzrelevanten Vorhaben (Vorabkontrollen) und nimmt Stellung zu Erlassen. Er bietet Aus- und Weiterbildungen in den Bereichen Datenschutz und Informationssicherheit an.

– Bei öffentlichen Organen überprüft er mittels Kontrollen (Datenschutzreviews), ob die Anforderungen des Datenschutzes in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht eingehalten sind.

– Der Datenschutzbeauftragte berät Privatpersonen über ihre datenschutzrechtlichen Ansprüche und vermittelt in Konfliktfällen zwischen Privatpersonen und öffentlichen Organen. Er informiert die Öffentlichkeit über die Anliegen des Datenschutzes und der Informationssicherheit.

Inhaltsverzeichnis

Überblick

Konsequenter Datenschutz braucht Ressourcen

Im Jahr 2018 hat der Regierungsrat die Strategie «Digitale Verwaltung 2018 – 2023» verabschiedet und mit einem Impulsprogramm zusätzliche finanzielle und personelle Mittel für eine rasche Umsetzung gesprochen. «Konsequent digital» heisst die neue Vorgabe für die Verwaltung. «Datenschutz, aber konsequent» ist das Pendant, für das sich der Datenschutzbeauftragte auch bei der Digitalisierung einsetzt.

Auch die digitalen Bürgerinnen und Bürger wollen, dass die Verwaltung ihre Daten schützt. Eine 2018 von der ZHAW im Auftrag der Staatskanzlei und des Vereins der Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV) durchgeführte Studie[1] zeigt, dass die Bevölkerung bei E-Services das Merkmal «Datensicherheit und Datenschutz» neben dem Preis als sehr wichtig einstuft. Die Bedeutung von Datenschutz und Datensicherheit wird dabei umso stärker gewichtet, je vertraulicher die Daten sind.

Tatsächlich bearbeitet die Verwaltung nicht nur eine riesige Menge an Daten, sondern auch immer mehr sehr sensitive Daten. Davon sind alle Bürgerinnen und Bürger betroffen – im Gesundheitswesen oder im Bildungsbereich. Sensitiv sind aber auch die Datenbearbeitungen im Bereich des Kindes- und Erwachsenenschutzes oder bei der Polizei und der Strafverfolgung. Der Datenschutzbeauftragte beschäftigte sich 2018 mit einer grossen Anzahl an Fragen aus diesen Gebieten (Seite 18).

Herausforderung Datensicherheit

Kontrollen und Prüfungen in unterschiedlichen Verwaltungsbereichen, bei Gemeinden, Spitälern und bei IT-Dienstleistern für die Verwaltung zeigten, dass die Sicherheit der Daten in der Digitalisierung eine grosse Herausforderung darstellt. Bis jetzt konnte noch keine nachhaltige Verbesserung der Informationssicherheit bei den öffentlichen Organen festgestellt werden (Seite 23).

Dabei wird der Austausch der Daten – auch über die Landesgrenzen hinweg – zur Selbstverständlichkeit: Verwaltungen speichern ihre Daten in der Cloud und nehmen Dienstleistungen in Anspruch, die in der Cloud erbracht werden. Die rechtlichen, organisatorischen und technischen Massnahmen zum Schutz der Daten sind komplex und oft ist es schwierig, mit allen Dienstleistern die offenen Fragen zu besprechen. Teilweise nutzen öffentliche Organe Standardprodukte wie Messenger-Dienste, ohne sich Gedanken zu machen über die damit zusammenhängenden Fragen des Datenschutzes und der Datensicherheit (Seite 30).

[1] Zürcher Hochschule für Angewandte Wissenschaften (ZHAW), Bedarfserhebung Digitales Leistungsportfolio bei Zürcher Gemeinden, Winterthur 2018 (ISBN 978-3-03870-023-4).

Schutz der Freiheitsrechte

Bei der Konzipierung der Digitalstrategie wie auch bei den in die Wege geleiteten Gesetzesrevisionen wird der Schutz der Freiheitsrechte der Bürgerinnen und Bürger zu wenig berücksichtigt (Seite 36). Die digitale Verwaltung ist aber auf das Vertrauen der Bürgerinnen und Bürger angewiesen. Ihr Vertrauen gründet auf dem Schutz ihrer Privatsphäre, also dem Datenschutz und dem sicheren Umgang mit ihren Daten.

Der Einsatz des Datenschutzbeauftragten für die Grundrechte der Bevölkerung stösst aber an Grenzen. Er kann die gesetzlichen Aufgaben mit den heutigen Ressourcen überall nur zum Teil wahrnehmen. Die Nachfrage nach Beratungen übersteigt die Möglichkeiten der Behörde und in Projekten und bei Ausbildungstätigkeiten kann er nur beschränkt mitwirken. Seit Jahren fehlen die Ressourcen für eine nachhaltige Kontrolltätigkeit, obwohl sich immer wieder grosse Lücken bei der Informationssicherheit zeigen. Das Plenum des Kantonsrats hat in der vergangenen Legislaturperiode eine Ressourcenaufstockung trotzdem zweimal abgelehnt.

Datenschutzaufsicht beim SIS

Das Schengen-Informationssystem (SIS) ist das Fahndungssystem der EU. Die Schengen-Assoziierung ermöglicht seine Nutzung auch den Schweizer Polizeien, auch im Kanton Zürich. 2018 wurden über 19 000 Treffer mit Bezug zur Schweiz registriert. Ohne SIS wäre die Schweizer Polizei blind, bemerkte ein Vertreter der Bundespolizei. Die erfolgreichen Fahndungssysteme brauchen auch einen klaren datenschutzrechtlichen Rahmen. Die EU als Eigentümerin des SIS evaluiert in den angeschlossenen Ländern regelmässig, ob die datenschutzrechtlichen Vorgaben eingehalten werden. Die Evaluation in der Schweiz im Jahr 2018 hat zu verschiedenen Empfehlungen in Bezug auf die Datenschutzbehörden geführt, für deren Umsetzung die Schweiz einen Aktionsplan erstellen muss. Die Empfehlungen verlangen, dass die Durchsetzungsbefugnisse der Datenschutzbehörden gestärkt werden. Ihnen soll das Recht verliehen werden, direkt rechtsverbindliche Entscheidungen zu treffen.

Ebenso wird verlangt, dass den Datenschutzbehörden ausreichende finanzielle und personelle Mittel zur Verfügung gestellt werden, damit sie ihre Kontrollaufgaben im Rahmen des SIS wahrnehmen können. Dabei geht es um eine regelmässige Kontrolle der Rechtmässigkeit der Datenbearbeitungen im SIS.

Mit der Revision des Informations- und Datenschutzgesetzes (IDG) sollen im Kanton Zürich die Kompetenzen des Datenschutzbeauftragten gestärkt werden (Seite 37). Aufgrund mangelnder Ressourcen konnte in den letzten zehn Jahren im Kanton Zürich nur eine einzige Kontrolle der Datenbearbeitungen im SIS durchgeführt werden.

Digitalisierung braucht Ressourcen

Die Verwaltungsausgaben für die Datenbearbeitungen sind in den letzten Jahren stetig gestiegen. Der Regierungsrat stellt für die Verwaltung zusätzliche personelle Ressourcen und finanzielle Mittel in Millionenhöhe zur Verfügung, um der Digitalisierung den notwendigen Schub zu verleihen. Es ist nicht konsequent, wenn der Kantonsrat einerseits diese Aufstockungen genehmigt und andererseits die Anliegen eines angemessenen Datenschutzes ablehnt.

Ohne zusätzliche Ressourcen für den Datenschutzbeauftragten – dem Kompetenzzentrum für Datenschutz des Kantons Zürich – wird die Digitalisierung aber zu einem nicht einschätzbaren Wagnis für die Bürgerinnen und Bürger. Die Informatiksysteme werden komplexer und die Abhängigkeit von der Informationstechnologie nimmt zu, was die Cyberrisiken und die Gefahr des Missbrauchs von persönlichen Daten und digitalen Identitäten wachsen lässt. Die notwendigen Risikoabschätzungen werden nicht vorgenommen und die Technologien kaum auf ihre Datenschutzfreundlichkeit geprüft. Vorabkontrollen bei der Planung von Datenbearbeitungen und Kontrollen von bestehenden System sind Präventionsmassnahmen und gehören zu den Aufgabenfeldern des Datenschutzbeauftragten. Dieser präventive Datenschutz ist aktuell aber nicht gewährleistet.

Defizite in der Aufgabenerfüllung

Das Jahr 2018 hat gezeigt, dass der Datenschutzbeauftragte die neue Dynamik der Digitalisierung nicht ohne Weiteres aufnehmen kann. Um in diesem Bereich die datenschutzrechtlichen Interessen der Bürgerinnen und Bürger geltend machen zu können, braucht es einen umfassenden Check-and-Balances-Prozess: Rechtliche, organisatorische und technische Anforderungen zum Schutz der Daten und ihrer Sicherheit müssen rechtzeitig und angemessen in die Digitalisierungsprojekte eingebracht werden können.

So liegt die Priorität auch beim Datenschutzbeauftragten im Bereich der Digitalisierung. Hier fallen heute die Entscheidungen darüber, wie die Verwaltung die Daten der Bürgerinnen und Bürger in Zukunft bearbeiten wird. Dabei müssen auch die Sicherung von Grundrechten und die Einhaltung gesetzlicher Bestimmungen zu den Zielvorgaben gehören. Dafür muss der Datenschutz von Anfang an mitgedacht werden. Doch die Konzentration auf die Digitalisierungsfragen darf nicht dazu führen, dass all die übrigen Datenbearbeitungen in der Verwaltung keine datenschutzrechtliche Begleitung mehr erhalten.

Die erwähnte Studie zeigt: Die Erwartungen der Bevölkerung in Bezug auf den Schutz und die Sicherheit ihrer vom Staat bearbeiteten Daten sind eindeutig. Es liegt an der Politik, die richtigen Weichen zu stellen.

Leistungsindikatoren im KEF

Die für das Jahr 2018 festgelegten Indikatoren im Konsolidierten Entwicklungs- und Finanzplan (KEF) weisen auf eine zunehmende Überlastung der Kapazitäten des Datenschutzbeauftragten hin.

Mit den bestehenden Ressourcen können etwa 500 Beratungen pro Jahr durchgeführt werden. Dieser Wert wurde 2018 um 20 Prozent überschritten. Die Beratungen im Kontext mit Digitalisierungsprojekten der Verwaltung werden zudem anspruchsvoller und aufwendiger. Die hohe Leistungsbereitschaft der Mitarbeitenden ermöglichte es, diesen Zusatzaufwand zu leisten. Um die Bedürfnisse der öffentlichen Organe und der Bürgerinnen und Bürger auch in diesem Bereich in Zukunft erfüllen zu können, braucht der Datenschutzbeauftragte zusätzliche Ressourcen.

Mit einem Monitoring stellt der Datenschutzbeauftragte sicher, dass er bei allen massgeblichen Vernehmlassungen einbezogen wird. Bei dieser Messgrösse wird von einer Mischung aus mehr oder weniger zeitaufwendigen Vernehmlassungsvorlagen ausgegangen. Im Berichtsjahr erfolgten quantitativ weniger Vernehmlassungen, dafür war zu Vorlagen von grosser Bedeutung Stellung zu nehmen, wie der IDG-Revision, der Totalrevision des Sozialhilfegesetzes oder den Leitlinien der Konferenz der Kantonsregierungen (KdK) zur Digitalen Verwaltung. Ihre Bearbeitung beanspruchte entsprechend viele Ressourcen.

Der Datenschutzbeauftragte bietet zahlreiche Weiterbildungen an, oft in Zusammenarbeit mit Ausbildungspartnern. Im Rahmen einer Zusammenarbeit mit der ZHAW werden verschiedene Seminare durchgeführt. Weitere Kurse, Seminare und Referate ergänzen diese Aktivitäten. Im Jahr 2018 ist der neue CAS Datenschutzverantwortliche an der ZHAW besonders zu erwähnen.

Aufgrund mangelnder Ressourcen kann die Kontrolltätigkeit nicht im vorgesehenen Ausmass durchgeführt werden. In der ersten Jahreshälfte erfolgten Nachkontrollen und in der zweiten Jahreshälfte wurden mehrere vertiefte Datenschutzreviews gestartet, die mit grösserem Aufwand verbunden sind.

Die Indikatoren zeigen, dass die gesetzlichen Aufgaben des Datenschutzbeauftragten kurz- und mittelfristig nur mit zusätzlichen Ressourcen zu bewältigen sein werden. Die umfassende Digitalisierung der Verwaltung in den nächsten Jahren wird zudem zu einer stark steigenden Nachfrage nach den Dienstleistungen des Datenschutzbeauftragten wie Beratung und Vorabkontrollen führen. Gerade vor dem Hintergrund der fortschreitenden Digitalisierung bleiben auch die übrigen gesetzlichen Aufgaben wie Information sowie Aus- und Weiterbildung wichtig.

Leistungsindikatoren		KEF	2018
Beratungen	Der DSB berät öffentliche Organe und Privatpersonen in Fragen des Datenschutzes und der Informationssicherheit. Die Beratung erfolgt persönlich, telefonisch, per E-Mail oder Brief. Der Leistungsindikator im KEF misst die getätigten Beratungen von Privatpersonen.	500	600
Vernehmlassungen	Der DSB beurteilt Entwürfe von Erlassen und Vorhaben im Gesetzgebungsverfahren mit Bezug zu Datenschutz und/oder Informationssicherheit. Dazu verfasst er Vernehmlassungsantworten, Stellungnahmen und Mitberichte. Der Leistungsindikator im KEF gibt Auskunft über die eingereichten Vernehmlassungsantworten, Stellungnahmen und Mitberichte.	18	14
Weiterbildung und Information	Der DSB bietet Aus- und Weiterbildungen im Bereich des Datenschutzes und der Informationssicherheit an. Dies erfolgt in der Form von internen oder externen Seminaren, Kursen, Workshops, Web-Trainingsprogrammen und Referaten. Der Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote für öffentliche Organe.	20	30
Kontrollen	Der DSB kontrolliert die Anwendung der rechtlichen, technischen und organisatorischen Vorschriften über den Datenschutz und die Informationssicherheit durch die öffentlichen Organe. Dazu führt er Datenschutzreviews, Kontrollen auf Anlass sowie technische Kontrollen durch. Der Leistungsindikator im KEF gibt Auskunft über die realisierten Kontrollen.	40	25

Sensibilisierung

Die Herausforderungen der Digitalisierung diskutieren

Der Datenschutzbeauftragte fördert mit seinen Veranstaltungen die Diskussion über die Auswirkungen der Digitalisierung auf die Grundrechte, die demokratische Gesellschaftsordnung und den Rechtsstaat. Er sucht nach Lösungen, wie die technologische Entwicklung menschenfreundlich gestaltet werden und wie die persönliche Freiheit auch in Zukunft geschützt werden kann.

Das IDG definiert als Auftrag des Datenschutzbeauftragten, die Öffentlichkeit über die Anliegen des Datenschutzes zu informieren. Er achtet darauf, für jede Zielgruppe die wirkungsvollste Umsetzung zu finden und die Bedeutung des Schutzes der Privatsphäre, des Datenschutzes und der Informationssicherheit in unterschiedlichen Umfeldern zu thematisieren. Im Fokus standen 2018 neben den Fachleuten aus Politik und Verwaltung besonders die Schulkinder, die in die digitale Welt hineinwachsen, Jugendliche, deren Aktivitäten massgeblich über soziale Medien ablaufen, sowie politische, gesellschaftliche und kulturelle Macherinnen und Macher.

Von Kindesbeinen an selbstbestimmt digital unterwegs

Der Datenschutzbeauftragte erarbeitete zusammen mit der Pädagogischen Hochschule Zürich (PHZH) Unterrichtsmaterialien für Schulkinder des Zyklus 1 des Lehrplans 21. Unter dem Titel «Geheimnisse sind erlaubt» erfahren schon Vierjährige anhand eines Zeichentrickfilms, dass die gleiche Information in verschiedenen Umfeldern sehr unterschiedliche Bedeutungen haben kann. In fünf Lektionen lernen die 4- bis 9-jährigen Kinder, warum es wichtig ist, wer was über sie weiss, welche Geheimnisse sie besser für sich behalten und wann eine erwachsene Vertrauensperson beigezogen werden soll. Sie verstehen, welche Informationen sich für den privaten, den halböffentlichen oder eben den öffentlichen Raum und damit etwa das Internet eignen und dass vermeintlich harmlose Einzelstücke von Informationen viel über eine Person aussagen können, wenn sie verknüpft werden.

Die besondere Herausforderung bei der Erarbeitung dieses neuartigen Lehrmittels lag darin, die komplexen Themen für die Kleinsten erfassbar zu machen. Durch die Vielfalt der verwendeten methodischen Ansätze können die Lehrpersonen die Materialien in unterschiedlichen Umfeldern einsetzen. Die Kinder begreifen dadurch, dass der Schutz der Privatsphäre in den verschiedensten Lebensbereichen wichtig ist.

Die PHZH testet die Lektionen an Schulen und integriert das Lehrmittel ab Herbst 2019 in die Lehrpersonen-Ausbildung. Die Unterrichtseinheiten für den Zyklus 1 sind als E-Book kostenlos verfügbar und können ohne grossen Aufwand überall eingesetzt werden. In den nächsten zwei Jahren werden Unterrichtsmaterialien für die Zyklen 2 und 3 erstellt. Damit erreicht der Datenschutzbeauftragte dank der Zusammenarbeit mit der PHZH eine nachhaltige Integration der persönlichkeitsbildenden Inhalte über das gesamte Schulcurriculum hinweg.

Junge Videoschaffende reflektieren über ihre eigene Welt

Der Datenschutz-Video-Wettbewerb fand 2018 zum dritten Mal statt, diesmal unter dem Titel Gläserner Mensch – Wer weiss was über mich? Eine Jury, der neben dem Datenschutzbeauftragten Mitglieder aus den Bereichen Medienbildung, Kultur und Videoproduktion sowie der Gewinner des vorjährigen Wettbewerbs angehörten, konnte aus einer grossen Vielfalt von Beiträgen auswählen. Kleine Spielfilme waren ebenso dabei wie klassische Youtube-Videos oder Produktionen mit Performance-Charakter.

Der Gewinner des letztjährigen Datenschutz-Video-Wettbewerbs, Gian Maria Finger, moderierte die Preisverleihung am Digital Festival. Die Wettbewerbsteilnahme habe ihn weiter für das Thema sensibilisiert, meinte er, wenn Google seine Suchanfragen heute automatisch richtig erweitere, fände er das ziemlich krass. Er frage sich dann: Was wissen die sonst noch über mich?

Das Gewinnertrio will mit seinem Beitrag Nutzen und Risiken von Gesundheitsdaten dazu anregen, sich zu informieren und mitzureden, wie es im Abspann ihres Videos heisst. Sie zeigen den Alltag eines jungen Mannes, dessen Daten ununterbrochen aufgezeichnet und ausgewertet werden. Er bekommt aufgrund dieser Datenanalyse ungefragt Tipps zur Verbesserung seiner Gesundheit, Warnungen zu seinem Verhalten und letztendlich wird die Krankenkassenprämie seinem Risiko-Lifestyle als ziemlich durchschnittlichem Zürcher nach oben angepasst. Es entstand ein «spannender Kurzfilm, der zum Nachdenken anregt, ohne moralisch zu sein», wie die Jury befand. Der zweitplatzierte Beitrag Daten.Wir greift die Thematik des Zauberlehrlings auf, der dank einer Datenbrille seine Umgebung manipulieren kann, weil er die Träume und Ängste seiner Freundinnen und Freunde aufgrund ihrer Spuren im Internet kennt. Ein verführerischer Wunsch – bis er merkt, wie das Vertrauen verloren geht und ohne Vertrauen das Zusammenleben unmöglich wird. Auf dem dritten Platz landete der Clip zersch überlegge. Er macht auf eindringliche Art deutlich, wie unsere eigenen Beiträge in sozialen Medien sich gegen uns wenden können.

Mit dem Datenschutz-Video-Wettbewerb bekommen Jugendliche und junge Erwachsene die Möglichkeit, über den Schutz der Privatsphäre in ihrer digitalen Welt zu reflektieren und zu diskutieren. Sie verwenden die Sprache des Mediums und die Inhalte gewinnen bei der Zielgruppe an Glaubwürdigkeit, weil sie von Peers stammen. Dadurch sind die Videos für Workshops in der Jugendarbeit und in den Schulen geeignet. Sie sind auf dem Youtube-Kanal des Datenschutzbeauftragten publiziert.

Entscheiden Big Data und Künstliche Intelligenz die Wahlen 2019?

«Die Wahlen 2019 werden durch Menschen entschieden», beruhigte Martin Künzi, Mitinhaber der Digitalmarketingagentur Enigma, am Expertengespräch des Symposium on Privacy and Security. Eine Abstimmung mit Umfrageresultaten von 55 zu 45 Prozenten könne er allerdings mit Mikrotargeting kippen, meinte er. Für seinen Konkurrenten Thomas Hutter von Hutter Consult ist es deshalb zentral, die Werbekunden anzuleiten: «Nur weil mir eine Plattform eine Möglichkeit anbietet, heisst das noch lange nicht, dass es erlaubt ist, diese Möglichkeit zu nutzen.»

Die eidgenössischen und kantonalen Datenschutzbehörden haben 2018 gemeinsam einen Leitfaden mit Vorgaben für die Datennutzung bei der politischen Online-Kommunikation erarbeitet.

Demokratie ohne Privatsphäre undenkbar

«Es besteht die Gefahr, dass wir die Demokratie an Private verkaufen», sagte Moritz Riesewieck, Regisseur des Dokumentarfilms The Cleaners am ZFF Talk zum Thema #BigData – Das Ende der Selbstbestimmung? Unter der Leitung des NZZ-Redaktors Stefan Betschon diskutierten neben Riesewieck auch Monika Dommann, Historikerin der Universität Zürich, und Bruno Baeriswyl unter anderem über Fragen zur Aufgabenverteilung zwischen Privatwirtschaft und Staat. Der Film The Cleaners berichtet über die Tausenden von Mitarbeitenden unabhängiger Firmen auf den Philippinen, die alle Inhalte anschauen und beurteilen, die weltweit auf eines der sozialen Netzwerke von Facebook über Twitter bis Youtube geladen werden. Sie entscheiden, welche Äusserungen, Bilder und Filme in den Timelines der Nutzerinnen und Nutzer erscheinen – und welche unbemerkt gelöscht werden. «Wir dürfen die Öffentlichkeit nicht privatisieren», meinte Bruno Baeriswyl. Demokratie sei ohne Privatsphäre nicht denkbar. Konkret hätten dies die Hinweise auf Wahlbeeinflussung auf Plattformen der sozialen Medien deutlich gemacht.

Entscheiden, welche Zukunft wir wollen

Der Datenschutzbeauftragte organisierte zusammen mit dem Helmhaus der Stadt Zürich eine Diskussion darüber, wie wir unsere Zukunft selbst bestimmen können angesichts der Entwicklung von Künstlicher Intelligenz und selbstlernenden Algorithmen. Im Rahmen der Ausstellungstrilogie Refaire le monde besprachen die Medienpsychologin Sarah Genner, der ETH-Professor Ueli Maurer und Bruno Baeriswyl unter der Leitung der Tages-Anzeiger-Chefredaktorin Judith Wittwer mögliche Zukunftsszenarien angesichts der fortschreitenden technologischen Entwicklungen. Wittwer stellte Tobi vor, die Künstliche Intelligenz, die beim Tages-Anzeiger mitschreibt. Ueli Maurer stellte klar: «Die Digitalisierung ist keine Revolution. Es ist eine Explosion. Und wo die Teilchen davon landen, das wissen wir heute nicht.» Er wies darauf hin, dass die Softwarebranche als einzige keine Haftpflicht kenne. Wäre dies anders, würden wir heute in einer sichereren Umwelt leben, meinte er. Sarah Genner hob hervor, dass eine der wichtigsten Aufgaben des Bildungssystems gerade in Zeiten der Digitalisierung sei, das kritische Denken zu fördern. Letztendlich, so Baeriswyl, sei es an den Menschen zu entscheiden, wie sie leben wollten. Die Frage sei: «Wollen wir in einer Demokratie leben, ja oder nein?»

Im Takt der Algorithmen

Das 23. Symposium on Privacy and Security stellte die Frage, ob Künstliche Intelligenz und Digitalisierung Chance oder Schicksal für die Gesellschaft seien. Geben Mensch oder Algorithmen den Takt an? Algorithmen werden zwar noch von Menschen geschrieben, aber sie lernen und entwickeln sich selbstständig weiter. Die Künstliche Intelligenz ist eine neue Herausforderung in Wirtschaft und Verwaltung, aber auch generell für unsere Gesellschaft.

Es sei eine Illusion, die Lösungen der Künstlichen Intelligenz nachvollziehbar machen zu wollen, meinte Joachim M. Buhmann, Professor für Computerwissenschaft an der ETH. Die Veränderungen, welche die Künstliche Intelligenz mit sich bringe, seien vergleichbar mit der Nutzbarmachung des Feuers durch den Menschen. Der Mensch müsse sich auf seine Fähigkeiten besinnen, denn er sei mehr als eine Rechenmaschine. Jana Koehler, Professorin an der Hochschule Luzern, äusserte ihre Überzeugung, dass eine demokratische und humanistische Gesellschaft die neue Technologie vernünftig einsetzen und dank ihr ein ausgewogeneres Verhältnis zu ihrem Planeten entwickeln könne. Mike Weber vom Kompetenzzentrum Öffentliche IT des Fraunhofer Instituts stellte aktuelle Anwendungen Künstlicher Intelligenz in der Verwaltung vor, etwa in der Korruptionsbekämpfung, der Verkehrssteuerung oder der Krisenfrüherkennung. Die grundsätzliche Frage sei, wer die Verantwortung trage: «Wenn der Mensch nur noch Entscheidungsunterstützung leistet, geraten wir in Probleme.» Der öffentliche Bereich brauche vielleicht eine andere, regelbasierte Künstliche Intelligenz.

Datenschutz-kompetenz dank Weiterbildung

Bürgerinnen und Bürger erwarten von der Verwaltung, dass mit ihren Daten und Informationen korrekt umgegangen wird. Die Risiken für Datenmissbräuche und Datenlecks nehmen jedoch ständig zu. Die Bevölkerung hat grosses Vertrauen in den Staat, wie Umfragen immer wieder bestätigen. Eine fundierte Datenschutzkompetenz der Verwaltung und Behörden trägt dazu bei, das Vertrauen zu erhalten.

Mitarbeiterinnen und Mitarbeiter von öffentlichen Organen in Kanton und Gemeinden müssen mit Personendaten gesetzeskonform umgehen können. Die Einhaltung des Datenschutzes ist ein Qualitätsmerkmal für alle Verwaltungsbereiche. Das Weiterbildungsangebot des Datenschutzbeauftragten soll die notwendigen Handlungskompetenzen fördern und verbessern.

In allen Fällen sind die Anforderungen des IDG umzusetzen. Das öffentliche Organ muss die Dienste sorgfältig auf die datenschutzrechtlichen Anforderungen überprüfen. Der Leitfaden Bearbeiten im Auftrag des Datenschutzbeauftragten beinhaltet Checklisten und Übersichten für das Vorgehen, die Vertragsbestimmungen und die zu implementierenden Informationssicherheitsmassnahmen.

Zusammenarbeit mit der ZHAW

Der Datenschutzbeauftragte gründete 2015 zusammen mit der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) das Zürcher Zentrum für Informationstechnologien und Datenschutz (www.itpz.ch). Daraus hat sich ein etabliertes und nachhaltiges Weiterbildungsangebot für die Verwaltung entwickelt. In Seminaren und Kursen werden Grundlagen vermittelt, Fälle aus der Praxis gelöst und aktuelle Fragen der Teilnehmenden diskutiert. Die Teilnehmenden profitieren voneinander, indem bei Fragen verschiedene Lösungsansätze aufgezeigt und einander gegenübergestellt werden. Der Fokus des Kursangebots liegt auf Bereichen, in denen sensitive Datenbearbeitungen stattfinden (Sozialbereich, Gesundheitswesen, Kindes- und Erwachsenenschutz) oder Risiken durch Technologien zunehmen (medizinische Forschung, Digitalisierung). Auf Anfrage werden auch Kurse und Seminare für Verwaltungsstellen und Institutionen angeboten.

CAS Datenschutzverantwortliche erstmals durchgeführt

Der Zertifikatskurs CAS Datenschutzverantwortliche ist ein Meilenstein in der Zusammenarbeit des Datenschutzbeauftragten und der ZHAW. Er wurde von beiden Institutionen gemeinsam konzipiert und ab Sommer 2018 durch die ZHAW erstmalig angeboten. In einem kompakten Lehrgang von rund vier Monaten werden Kompetenzen in Datenschutzrecht, IT-Risiken und Informationssicherheit, Information Governance, Datenschutz-Compliance und Datenschutz-Management vermittelt.

Weitere Angebote

Neben dem eigenen Kursangebot des ITPZ nimmt der Datenschutzbeauftragte auch Dozentenengagements in Lehrgängen von Bildungsinstitutionen wahr. In Modulen von wenigen Lektionen bis ein oder zwei Unterrichtstagen werden Datenschutzkompetenzen vermittelt.

- Seminare und Kurse: Datenschutz im Sozialbereich, Datenschutz im Gesundheitswesen, Datenschutz und Öffentlichkeitsprinzip
- Mitwirkung in Lehrgängen: CAS Kindes- und Erwachsenenschutzrecht, CAS Sozialhilferecht, beide ZHAW; CAS Clinical Trial Management, Europa-Seminare, beide UZH; Datenschutzkurs für Informatiker, HSR

Sensitive Daten

19 Zunehmend sensitive Datenbearbeitungen

Zunehmend sensitive Datenbearbeitungen

Öffentliche Organe bearbeiten eine Vielzahl von sensitiven Daten, beispielsweise im Gesundheitswesen, im Kindes- und Erwachsenenschutz oder im Bereich Strafverfolgung und Strafvollzug. Die Einhaltung der datenschutzrechtlichen Rahmenbedingungen bildet die Voraussetzung zur Gewährleistung der Grundrechte und dient dem Funktionieren des demokratischen Staates. Dies gilt auch im digitalisierten Zeitalter, in dem die Menge der Daten rasant wächst und ihre Weiterverwendung immer einfacher wird.

Herausforderung Anonymisierung von Gesundheitsdaten

Der Datenschutzbeauftragte befasste sich mit vielen Anfragen, die Datenbearbeitungen in sensitiven Bereichen betreffen. Ein Schwerpunkt bildete der Bereich der medizinischen Forschung. Die Forschung mit Gesundheitsdaten kann zu neuen Erkenntnissen über die Behandlung von Krankheiten und ihrer Prävention führen. Sie birgt ein enormes Potenzial für die Wirtschaft. Das Interesse an der Datennutzung ist gross. Die medizinische Forschung beinhaltet aber auch Risiken für die Privatsphäre der betroffenen Personen.

Die Anonymisierung der Gesundheitsdaten steht hier im Fokus. Sie bietet für die Forschenden den Vorteil, dass ein Forschungsprojekt keiner Bewilligung der Ethikkommission bedarf. Der Datenschutzbeauftragte befasste sich vermehrt mit Anfragen zur Beurteilung des Anonymisierungsprozesses der Daten. Jedes Forschungsprojekt ist im Einzelfall zu beurteilen und die Anforderungen an die Anonymisierung sind hoch anzusetzen. Die Schwärzung respektive Löschung von identifizierenden oder identifizierbaren Angaben wie Name, Adresse, Geburtsdatum, AHV-Nummer, Patientenidentifikations- und Fallnummer reichen in der Regel nicht aus, um die Anonymität zu gewährleisten. Weitere Faktoren sind zu berücksichtigen, wie die restlichen in den Datensätzen enthaltenen Informationen, die auf die Datensätze zugriffsberechtigten Personen, die Kriterien zur Auswertung der Daten und die Anzahl betroffener Personen. Aufgrund des technologischen Fortschritts steigt das Risiko für die Re-Identifizierung von Personen durch den Abgleich oder die Verknüpfung der Daten mit weiteren Datenbeständen. Der Datenschutzbeauftragte fordert, dass keine Abgleiche oder Verknüpfungen durchgeführt werden. Er verfolgt das Thema aufmerksam, vor allem die Frage, ob in Zukunft die wirksame Anonymisierung von Gesundheitsdaten überhaupt möglich bleibt.

Schweizer Recht bei Forschung mit internationaler Beteiligung

Ein weiteres Thema für die medizinische Forschung war die Datenschutz-Grundverordnung der Europäischen Union (DSGVO), die am 25. Mai 2018 in Kraft getreten ist. An Forschungsprojekten sind oft Unternehmen der Pharmaindustrie beteiligt, die international tätig sind. Im internationalen Kontext bildet die DSGVO den neuen Datenschutz-Standard. Dies hat zu Anfragen zu ihrer Anwendbarkeit auf Forschungsprojekte geführt. Dem Datenschutzbeauftragten wurde die Frage gestellt, ob die Teilnehmenden nicht nur nach den Anforderungen des Humanforschungsrechts über ein Forschungsprojekt aufzuklären sind, sondern auch nach denjenigen der DSGVO.

Bei der Durchführung einer Studie in der Schweiz ist das Schweizer Recht anwendbar, bei der medizinischen Forschung das Humanforschungsrecht, das Bundesgesetz über den Datenschutz respektive das kantonale Datenschutzgesetz. Die Aufklärung der Forschungsteilnehmenden nach den Anforderungen der DSGVO ist nicht notwendig. Legen ein Pharmaunternehmen als Sponsor und ein Spital vertraglich fest, dass die DSGVO für das Forschungsprojekt massgebend ist, kann eine Zusatzinformation an die Forschungsteilnehmenden abgegeben werden. Sie muss jedoch mit den Anforderungen an die Einwilligung für die Teilnahme am Forschungsprojekt nach dem Humanforschungsrecht vereinbar sein. Der Datenschutzbeauftragte führte dazu Gespräche mit der Ethikkommission des Kantons Zürich und mit Swissethics, dem Verein der Schweizerischen Ethikkommissionen für die Forschung am Menschen.

Rechte und Pflichten bei einem Spitalaufenthalt

Der informierten Bürgerin respektive dem informierten Bürger kommt im digitalisierten Umfeld eine immer wichtigere Rolle zu. Der Datenschutzbeauftragte veröffentlicht deshalb auf seiner Website eine Vielzahl von Informationen und Hilfsmitteln, darunter neu die Broschüre «Meine Rechte und Pflichten – Informationen zum Spitalaufenthalt», die gemeinsam mit der Gesundheitsdirektion und dem Verband Zürcher Krankenhäuser herausgegeben wurde. Sie löst die frühere Broschüre «Patientendossier – Meine Rechte» des Datenschutzbeauftragten ab, deren Inhalte in die neue Publikation eingeflossen sind. Die neue Broschüre informiert die Patientinnen und Patienten über ihre Rechte und Pflichten, auch in Bezug auf den Datenschutz. Die Rechte reichen von der Aufklärung und der Selbstbestimmung über medizinische Eingriffe und Therapien über das Recht auf Besuche und Seelsorge bis zum Recht, selbst darüber entscheiden zu können, wer in welchem Umfang über die eigenen Patientendaten informiert werden darf. Neben Erklärungen zur Führung der Patientendokumentation, zum Einsichts- und Berichtigungsrecht sowie zur Weitergabe von Patientendaten an Dritte enthält die Broschüre auch Informationen zur Patientenverfügung, zur Vertretung bei medizinischen Massnahmen, zum Einbezug in Lehrveranstaltungen sowie zur Teilnahme an Forschungsprojekten. Der Datenschutzbeauftragte ist überzeugt, den Patientinnen und Patienten mit der Broschüre eine praktische Hilfestellung zu bieten, damit sie ihre Rechte kennen und ausüben können.

Weitergabe von Berichten von KESB und Schulen an das Migrationsamt

Auch die Kindes- und Erwachsenenschutzbehörden (KESB) und die Schulen bearbeiten sensitive Personendaten. Ihre Weitergabe an Dritte muss sich auf eine klare gesetzliche Grundlage stützen und verhältnismässig sein. Das neue Bundesgesetz über die Ausländerinnen und Ausländer und über die Integration und die zugehörige Verordnung beinhaltet eine solche Grundlage. Diese verpflichtet verschiedene Behörden zur Meldung von Entscheiden an das kantonale Migrationsamt, unter anderem die KESB und die Schulen. Die KESB sind verpflichtet, dem Migrationsamt die Kinder- und Erwachsenenschutzmassnahmen zu melden, die Ausländerinnen und Ausländer betreffen und die das Migrationsamt für seine Entscheide benötigt. Zweck der Meldepflicht ist, dass das Migrationsamt und die KESB die Entscheide koordinieren können. Die Meldepflicht betrifft Fälle, in denen Kinder betroffen sind und die Rechte der Inhaber der elterlichen Sorge beschränkt werden (Kindesschutz) oder die Handlungsfähigkeit der betroffenen Person eingeschränkt wird oder entfällt (Erwachsenenschutz).

Im Rahmen der Umsetzung der Meldepflicht stellte sich die Frage, in welchem Umfang die Meldung zu erfolgen hat, etwa ob die KESB dem Migrationsamt die integralen Entscheide oder lediglich das Dispositiv oder einen Dispositivauszug übermitteln müssen. Entscheide der KESB können sensitive Informationen wie Auszüge aus psychiatrischen Gutachten enthalten. Der Datenschutzbeauftragte ist der Ansicht, dass der Verhältnismässigkeit grosses Gewicht beizumessen und ein abgestuftes Vorgehen angezeigt ist. Dem Migrationsamt dürfen nur die Informationen weitergegeben werden, die für die Erfüllung seiner Aufgaben geeignet und erforderlich sind. In einem ersten Schritt reicht es, wenn die KESB dem Migrationsamt das Dispositiv eines Entscheids respektive den auf die Anordnung von Massnahmen beschränkten Dispositivauszug

zukommen lässt. Benötigt das Migrationsamt weitergehende Informationen, um einen ausländerrechtlichen Entscheid zu fällen und mit einem Entscheid der KESB zu koordinieren, kann es diese im Einzelfall amtshilfeweise anfordern. Das Migrationsamt muss dann gegenüber der KESB begründen, weshalb es die Informationen benötigt. Die KESB prüft das Amtshilfegesuch und entscheidet, ob und in welchem Umfang sie weitere Auskünfte erteilt oder Unterlagen herausgibt.

Die Schulbehörden müssen neu dem Migrationsamt Entscheide über definitive Schulausschlüsse von ausländischen Schülerinnen und Schülern melden. Von der Meldepflicht ausgenommen sind Ausschlüsse von Schülerinnen und Schülern, die sich nicht rechtmässig in der Schweiz aufhalten. Zweck der Meldepflicht ist, dass das Migrationsamt prüfen kann, ob ein besonderer Integrationsbedarf besteht. Der Verordnungsgeber geht davon aus, dass einem Schulausschluss Regelverstösse zugrunde liegen, die einen ungünstigen Integrationsverlauf nicht ausschliessen lassen. Besteht ein besonderer Integrationsbedarf, kann sich dies auf das Erteilen oder Verlängern der Aufenthaltsbewilligung auswirken.

Der Datenschutzbeauftragte ist auch hier der Auffassung, dass die Meldung so viele Informationen umfassen muss, dass das Migrationsamt abschätzen kann, ob der Schulausschluss in Bezug auf die Beurteilung der Integrationskriterien relevant ist. Das Migrationsamt ist über die Gründe, die zum Schulausschluss geführt haben, in zusammenfassender Form zu informieren. Benötigt das Migrationsamt zur Prüfung des besonderen Integrationsbedarfs weitergehende Informationen, kann es diese im Einzelfall amtshilfeweise bei der Schule anfordern.

Empfehlungen zum Umgang mit schulpsychologischen Informationen

Im Schulbereich bearbeiten vor allem die schulpsychologischen Dienste sensitive Personendaten. Der Umgang mit den Personendaten stellt die Schulpsychologinnen und Schulpsychologen im Alltag vor grosse Herausforderungen. Der VSKZ (Vereinigte Schulpsychologinnen und Schulpsychologen des Kantons Zürich) hat Empfehlungen zum Umgang mit Personendaten in schulpsychologischen Diensten ausgearbeitet und dem Datenschutzbeauftragten zur Prüfung unterbreitet. Die Empfehlungen behandeln den Umgang mit Personendaten des schulpsychologischen Alltags und unterscheiden in Bezug auf Datenweitergaben, ob ein Verfahren läuft oder nicht, beispielsweise ein Rekursverfahren gegen einen Entscheid der Schulpflege oder ein Verfahren zu Kindesschutzmassnahmen der KESB. Der Datenschutzbeauftragte hat die Empfehlungen geprüft und verschiedene Hinweise und Ergänzungen angebracht. Der VSKZ hat diese berücksichtigt und die Empfehlungen im Januar 2019 publiziert.

Einsicht von Gemeinderäten in Mitarbeiterbeurteilungen

Die politischen Gemeinden bearbeiten sensitive Daten, beispielsweise im Rahmen der Mitarbeiterbeurteilungen (MAB). In einer Gemeinde entbrannte eine Diskussion zur Frage, ob die Behördenmitglieder Einsicht in die Unterlagen zu den MAB der einzelnen Gemeindemitarbeitenden erhalten dürfen. Sie wandte sich zur rechtlichen Klärung an den Datenschutzbeauftragten. Er wies darauf hin, dass das kantonale Personalrecht sinngemäss gilt, sofern die Gemeinde keine eigene Regelung aufgestellt hat. Er führte aus, dass die MAB der Förderung des Personals sowie der Beurteilung der Leistung und des Verhaltens und demzufolge der Personalführung dient. Nach dem Gesetz über die Information und den Datenschutz darf der Gemeinderat Personendaten bearbeiten, soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Der mit der Personalführung betraute Gemeinderat darf deshalb Einsicht in die Mitarbeiterbeurteilungen nehmen. Auch die Ressortvorsteherin oder der Ressortvorsteher kann in gewissen Fällen die Beurteilungen der Mitarbeitenden des Ressorts einsehen. Dies hängt im Einzelnen von den personalrechtlichen und organisatorischen Regelungen der Gemeinde ab. Im Einzelfall muss überprüft werden, ob die Einsichtnahme des Gemeinderates für die Aufgabenerfüllung, das heisst die Führungs- und Aufsichtsaufgaben, notwendig ist.

Videoüberwachung im Inneren einer Asylunterkunft

Fragen zu Videoüberwachungen bleiben aktuell. Der Datenschutzbeauftragte erhielt Kenntnis, dass eine Gemeinde plant, im Inneren einer Asylunterkunft Videokameras zu installieren und die Wohnräume zu überwachen. Als Grund für die Überwachungen wurden Vorfälle wie Sachbeschädigungen, Diebstahl und Aufenthalt von unbefugten Personen genannt.

Der Datenschutzbeauftragte beurteilt die Installation von Videokameras zur Überwachung von Wohnräumen als schweren Eingriff in das Grundrecht auf Schutz der Privatsphäre – sei es in einer Asylunterkunft oder einer anderen Wohninstitution. Aufgrund einer summarischen Prüfung gelangte er zur Einschätzung, dass die geplante Videoüberwachung der Gemeinde unverhältnismässig ist und den Kerngehalt des Grundrechts tangiert.

Electronic Monitoring: Beurteilung des Datenschutz- und Informationssicherheitskonzepts

Im Bereich der Strafverfolgung und des Strafvollzugs fallen grosse Mengen an sensitiven Daten an. Im Strafvollzug wird unter anderem Electronic Monitoring eingesetzt, das heisst die Überwachung von Personen mit elektronischen Geräten. Beispielsweise wird Electronic Monitoring zur Überwachung von verurteilten Personen angewendet, die während der Strafverbüssung ihre bisherige Arbeit fortsetzen und die Ruhe- und Freizeit im elektronisch überwachten Hausarrest verbringen. Als Überwachungsformen kommen Radiofrequenz- sowie GPS-Überwachungen zum Einsatz. Dabei fällt eine Vielzahl von Personendaten an und bei der GPS-Überwachung entsteht ein Bewegungsprofil der überwachten Person. Der Umgang mit diesen Daten wirft aus rechtlicher und organisatorisch-technischer Sicht Fragen auf. Das Amt für Justizvollzug hat ein umfassendes Datenschutz- und Informationssicherheitskonzept erarbeitet und dem Datenschutzbeauftragten zur Prüfung vorgelegt.

Der Datenschutzbeauftragte begrüsst die Schaffung des Konzepts und erachtet es als wichtige Hilfestellung für die beteiligten Behörden. Er nahm zu verschiedenen Punkten Stellung und gab Verbesserungsvorschläge ab. Die Arbeiten des Amts für Justizvollzug zur Überarbeitung des Konzepts sind noch im Gang.

Weitere Themen

Anforderungen an eine Einverständniserklärung zur Weitergabe von Informationen durch die Sozialberatung eines Spitals an Dritte: Für die Patientin oder den Patienten muss aus der Einverständniserklärung klar hervorgehen, wem zu welchem Zweck welche Informationen weitergegeben werden.

Buchprüfung in einer Arztpraxis durch das kantonale Steueramt: Der Arzt unterliegt der Mitwirkungspflicht und hat zugleich dafür zu sorgen, dass das Arztgeheimnis gewahrt bleibt. Um das Berufsgeheimnis zu wahren, sind die Unterlagen vorgängig zu anonymisieren.

Herausgabe schulpsychologischer Bericht durch den schulpsychologischen Dienst an die KESB: Die Herausgabe bedarf der Einwilligung der Eltern. Kann diese nicht eingeholt werden, kann der schulpsychologische Dienst die vorgesetzte Behörde um Entbindung von der Schweigepflicht ersuchen.

Angaben über den Gesundheitszustand für die Zulassung zur Ausbildung zum Bildungsgang Pflege FH: Die Pflicht zur Einreichung eines ärztlichen Zeugnisses an die Schulärztin respektive den Schularzt stützt sich auf eine gesetzliche Grundlage. In Bezug auf die Frage, welche Angaben anzugeben sind, verfügt die Bildungsinstitution über Ermessensspielraum. Die Kontrolle des Gesundheitszustandes von Personen, die im Pflegebereich arbeiten werden, ist aus Sicht des Patientenschutzes wichtig, etwa zur Verhinderung von übertragbaren Krankheiten durch nicht immunes Personal.

Bedrohte Personendaten

Mangelnder Schutz der Personendaten

Ein durchgängiger Mindeststandard bei der Informationssicherheit ist Voraussetzung für das Gelingen der Vorhaben der Digitalisierungsstrategie. Nur so kann den zunehmenden Risiken von immer ausgedehnteren Datenbearbeitungen und komplexeren Vernetzungen begegnet werden. Eine mangelnde Berücksichtigung des Datenschutzes bei der Umsetzung der Strategie Digitale Verwaltung gefährdet das aktuell ausgeprägte Vertrauen der Bürgerinnen und Bürger in den Staat.

Weiterhin Mängel in der Informationssicherheit

Der Datenschutzbeauftragte führte 2018 verschiedene Datenschutzreviews durch bei Gemeinden, Spitälern und IT-Dienstleistern sowie Checks von Websites, um die Einhaltung der Anforderungen beim Datenschutz in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht zu beurteilen. Diese Kontrollen zeigten, dass bei allen geprüften Organen weiterhin Mängel in der Informationssicherheit bestanden und im Kanton noch kein einheitliches und ausreichendes Sicherheitsniveau besteht.

Neu wurde 2018 ein Nachkontrollprozess eingeführt, womit die Wirkung der durchgeführten Kontrollen zeitnah und vertieft evaluiert werden kann. Dafür wird die Umsetzung monatlich kontrolliert, indem die geprüften Organe mit einem Schreiben auf die fälligen Massnahmen hingewiesen werden.

Damit reagierte der Datenschutzbeauftragte auf die Erkenntnis, dass bislang der Umsetzungsgrad bei Massnahmen, die bei früheren Kontrollen empfohlen worden waren, bei etwa 50 Prozent lag. Viele Organe hatten Schwierigkeiten, die Massnahmen inhaltlich und terminlich zufriedenstellend umzusetzen. Darunter befanden sich überraschend viele grössere Institutionen wie Spitäler, die über eigene und grössere IT-Abteilungen verfügen. Massnahmen, die grössere konzeptionelle Arbeiten und Änderungen bedingen, wurden während Jahren nicht in Angriff genommen und können jetzt nur schwer nachgeholt werden.

Vielfalt der Institutionen verlangt individuelle Vorgehensweisen

Der Datenschutzbeauftragte hat Massnahmen ergriffen, um die Wirkung seiner Kontrolltätigkeit zu verstärken. Trotzdem reichen die zur Verfügung stehenden Ressourcen im juristischen wie im technischen Bereich nicht zur Erfüllung des gesetzlichen Prüfauftrags. Der Datenschutzbeauftragte erbringt als einzige Instanz die Aufgaben von Prüfungen oder Revisionen der allgemeinen Informationssicherheit innerhalb der kantonalen Verwaltung und vor allem auch bei den Gemeinden. Zwar führen auch die Finanzkontrolle und das Steueramt Revisionstätigkeiten im Bereich der Informationssicherheit durch, sie beschränken sich jedoch auf die entsprechenden Spezialbereiche und Organe.

Insgesamt fallen über 1000 Organe unter den Kontrollauftrag des Datenschutzbeauftragten. Dazu gehören neben den rund 165 Gemeinden alle kantonalen Direktionen und Ämter, die Spitäler, Alters- und Pflegeheime, Schulen aller Stufen, die KESB, Gerichte, selbstständige und unselbstständige Anstalten, RAV, Fachstellen und Auftragnehmer aus der Privatwirtschaft. Die Vielfalt der Institutionen bedeutet eine zusätzliche Beanspruchung der Ressourcen. Die unterschiedlichen Organisationsformen und die sehr breit gefächerten Aufgaben verlangen eine individuelle Einarbeitung und Vorgehensweise.

Nachhaltige Stärkung der Informationssicherheit

Aufgrund von Erkenntnissen aus Kontrollen in Schulen erstellte das Mittelschul- und Berufsbildungsamt (MBA) zusammen mit dem Datenschutzbeauftragten eine Sammlung von Dokumenten zur nachhaltigen Stärkung der Informationssicherheit, um einen allgemeinen Standard für den Datenschutz und die Informationssicherheit zu schaffen (siehe Tätigkeitsbericht 2016, S. 42). Die Unterlagen wurden 2016 und 2017 in verschiedenen Workshops zusammen mit drei Pilotschulen erarbeitet. In einem zweiten Schritt testeten die Pilotschulen 2018 die Praxistauglichkeit der Vorlagen und Dokumente und verbesserten sie. So entstanden Unterlagen, welche die Schulleitungen und die Informationssicherheitsverantwortlichen im Sinne des Management-Kreislaufs bei der Planung, Umsetzung, Überprüfung und Verbesserung der nötigen Massnahmen unterstützen.

Der Regierungsrat beschloss Anfang 2019, die Informatik der Mittel- und Berufsfachschulen gemäss der kantonalen Strategie zu zentralisieren. Dadurch sind die Verantwortlichkeiten für die Umsetzung einzelner Massnahmen neu zu klären. Danach können die vom Datenschutzbeauftragten mit dem MBA erarbeiteten Grundlagen und Vorgaben für die Informationssicherheit an allen Schulen umgesetzt werden.

Systematischer Schutz von bedrohten Personendaten

Der Datenschutzbeauftragte wurde eingeladen, Stellung zu nehmen zur Allgemeinen Informationssicherheitsrichtlinie des Kantons. Sie ist der erste Schritt für den Aufbau eines Informationssicherheits-Managementsystems (ISMS).

Die zunehmende Bedrohung etwa durch Cyberangriffe verlangt nach effizienten, flexiblen und effektiven Mitteln für den Schutz von Informationen, besonders von Personendaten. Ein ISMS stellt dafür universelle Methoden und Werkzeuge bereit. Die Norm ISO / IEC 27001 beschreibt das ISMS und definiert die nötigen Massnahmen anhand des Management-Kreislaufes Planung, Umsetzung, Überprüfung und Verbesserung.

Die wichtigsten Ziele eines ISMS sind:

- Festlegen der Informationssicherheitspolitik und der Sicherheitsorganisation durch die oberste Leitung eines öffentlichen Organs oder Unternehmens (Planung)
- Definieren der Prozesse zur Beurteilung und Behandlung von Informationssicherheitsrisiken (Planung)
- Umsetzen der definierten Massnahmen zur Reduktion der Informationssicherheitsrisiken (Umsetzung)
- Bewerten der Wirksamkeit der Massnahmen zur Risikoreduktion (Überprüfung)
- Sicherstellen einer kontinuierlichen Verbesserung der Informationssicherheit (Verbesserung)

Ein ISMS würde die Informationssicherheit im Kanton nachhaltig unterstützen und stärken. Der Datenschutzbeauftragte begrüsst das Vorhaben. Die Allgemeine Informationssicherheitsrichtlinie und das ISMS wurden noch nicht definitiv verabschiedet.

Elektronische Dokumentation medizinischer Untersuchungen

Ein öffentliches Organ gelangte an den Datenschutzbeauftragten mit einem Projekt, das zum Ziel hat, medizinische Untersuchungen in Zukunft nicht mehr auf Papier, sondern digitalisiert zu dokumentieren. Für dieses Projekt sind die datenschutzrechtlichen Grundlagen für die Verantwortlichkeiten beim Datenaustausch der involvierten Stellen zu berücksichtigen. Die Wahrung des Berufsgeheimnisses der involvierten Ärzte und der Informationssicherheit sind besonders zu beachten.

Der Betrieb der Lösung, die Wartung der Applikation und der Betrieb eines Statistikmoduls sollten an Dritte ausgelagert werden. Die vertragliche Regelung der Auftragsdatenbearbeitung wurde geprüft. Daten, die dem Berufsgeheimnis unterliegen, müssen bei einer Auslagerung verschlüsselt gespeichert und das Schlüsselmanagement muss vertraglich festgelegt werden.

Der Datenschutzbeauftragte hielt fest, dass bei der Auswertung der Daten die Anonymität der betroffenen Personen bei jedem Bearbeitungsschritt zu gewährleisten ist. Die Hinweise des Datenschutzbeauftragten flossen in die Umsetzung des Projekts ein.

Sicherheit von Patientendaten gewährleisten

Der Datenschutzbeauftragte führte während der letzten drei Jahre zehn Kontrollen von Klinikinformationssystemen (KIS) durch bei Spitälern, deren Grösse, Fachbereiche und Organisationsformen unterschiedlich waren. Bei jeder Kontrolle wurden rechtliche Aspekte und Fragen zu Organisation und Technik geprüft.

Medizinische Daten sind sensitiv und als besondere Personendaten eingestuft. Die Anforderungen an den Schutz der Daten und die Informationssicherheit sind erhöht.

Spitäler sehen sich nicht nur mit den üblichen Themen der Informationssicherheit konfrontiert. Weitere Herausforderungen sind:

- die grosse Anzahl Patientinnen und Patienten
- die vielen Mitarbeitenden mit unterschiedlichen Zugriffsbedürfnissen
- eine weitgehend öffentlich zugängliche Infrastruktur
- die Einbindung von Drittanbietern und Lieferanten

Die Prüfungen zeigten Bereiche mit besonderem Verbesserungspotenzial:

- Einhaltung rechtlicher Vorgaben zur Datenbeschaffung und Datenbearbeitung, wie Prozesse zur Gewährung des Auskunftsrechts, die Nachvollziehbarkeit von Datenbearbeitungen und der Schulung der Mitarbeitenden
- Aufbewahrung von Informationen sowie Löschung der Daten nach Ablauf der gesetzlichen Aufbewahrungsfrist
- Definition und Einforderung der vertraglichen Grundlagen, wie Gerichtsstand oder AGBs
- fehlende, lückenhafte oder nicht aktuelle Dokumentationen und Frameworks
- nicht der heutigen Bedrohungslage angepasste Passwortrichtlinien
- keine oder nur geringe Unterscheidungen von Zugriffsrechten der Mitarbeitenden auf Patientendaten
- keine systematischen und umfassenden Schulungsmassnahmen, um die Mitarbeitenden für Risiken und Schutzmassnahmen zu sensibilisieren
- Verwendung von produktiven Daten auf Testsystemen, ohne dass dabei die gleichen Schutzmassnahmen wie auf produktiven Systemen umgesetzt werden
- fehlende Verschlüsselung von gespeicherten oder über interne und externe Netzwerke übertragenen Daten
- fehlende Konzeption und Umsetzung einer Protokollierung von Datentransaktionen

Persönliche Daten im Internet frei einsehbar

Ein unsachgemässer Aufbau oder Betrieb einer Website kann zu Verletzungen von Datenschutz- oder Geheimhaltungsvorschriften führen. Sicherheitsmassnahmen müssen umgesetzt und periodisch kontrolliert werden.

Ein öffentliches Organ machte einschlägige Erfahrungen mit den Risiken des Betriebs einer Website. In der betroffenen Webapplikation waren persönliche Daten während rund dreier Wochen im Internet frei einsehbar. Die Lücke wurde von der Entwicklerin der Webapplikation nach Bekanntwerden umgehend geschlossen. Die betroffenen Personen wurden über den Vorfall nicht informiert. Der Datenschutzbeauftragte wurde durch die Medien auf die Datenpanne aufmerksam gemacht und führte eine Kontrolle durch.

Die Kontrolle zeigte Optimierungspotenzial sowohl ihm rechtlichen wie auch im organisatorisch-technischen Bereich. Der Datenschutzbeauftragte verlangte vom verantwortlichen Organ die Umsetzung von Massnahmen in folgenden Bereichen:

- Einbindung der AGB Auslagerung Informatikleistungen des Kantons Zürich in den Vertrag mit der Entwicklerin der Webapplikation respektive Ergänzung des Vertrags im Rahmen einer Vertragsverlängerung oder -erneuerung gemäss dem Leitfaden Bearbeiten im Auftrag des Datenschutzbeauftragten
- Überprüfung von kritischen Funktionen, bevor eine neue Version der Webapplikation aufgeschaltet wird
- Protokollierung von kritischen Applikations- und Systemereignissen, um die Nachvollziehbarkeit zu gewährleisten
- Überprüfung und Anpassung der Architektur der Webanwendung

Cookie-Warnungen aufgrund der DSGVO

Der Datenschutzbeauftragte stellte fest, dass mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union auch öffentliche Organe des Kantons Zürich auf ihren Websites Banner mit Informationen über die Verwendung von Cookies und Analysetools platzierten und die Einwilligung der Seitenbesucherinnen und -besucher einholten. Die DSGVO ist auf öffentliche Organe des Kantons Zürich, die ihre Dienstleistungen in der Schweiz erbringen, nicht anwendbar. Der Datenschutzbeauftragte informierte die betroffenen Organe, dass die Cookie-Warnungen nicht nötig seien.

Sorge um Passwörter

Sichere Passwörter schützen Daten. Eine Person bat den Datenschutzbeauftragten, zur Passwortrichtlinie eines kantonalen Internetportals Stellung zu nehmen. Der Datenschutzbeauftragte informierte das Organ über die Thematik.

Bei der Festlegung von Passwortrichtlinien sind der Stand der Technik sowie die Vorgaben von international anerkannten Institutionen wie dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) oder dem US-amerikanischen National Institute of Standards and Technology (NIST) zu berücksichtigen.

Folgende technischen Massnahmen führen zu besseren Passwörtern:

- Lange Passwörter und ganze Sätze ermöglichen
- Mit einer Passworthistorie verhindern, dass bei der Passwortänderung das aktuelle Passwort als neues Passwort gewählt wird
- Die Benutzerinnen und Benutzer bei der Wahl eines Passworts unterstützen: beispielsweise die Passwortstärke grafisch darstellen
- Prüfen, ob das Passwort oder Teile davon in einem Wörterbuch vorkommen
- Zwei-Faktor-Authentifizierung anbieten

Der Datenschutzbeauftragte bietet einen Passwortcheck an, mit dem die Qualität der eigenen Passwörter überprüft werden kann.

Kritische Sicherheitsrisiken in Webanwendungen

Immer mehr Dienstleistungen werden ins Internet verlagert. Neben den Vorteilen ergeben sich daraus auch Sicherheitsrisiken. Der Datenschutzbeauftragte führte 2018 seine Strategie weiter, Auftragnehmende zu kontrollieren. Er entwickelte ein Kontrollprogramm zur Überprüfung von Unternehmen, die Dienstleistungen wie die Bereitstellung und das Hosting von Websites, den Betrieb eines Content-Management-Systems (CMS) und Onlinedienste im Bereich E-Government anbieten. Das Prüfprogramm umfasst Fragen in den Bereichen Recht, Organisation und Technik und kombiniert international anerkannte Standards mit spezifischen Fragen des Datenschutzbeauftragten.

Der Datenschutzbeauftragte erstellte aufgrund der Erkenntnisse aus einer ersten Kontrolle folgenden Massnahmenkatalog:

- Die Verantwortung für den Datenschutz und die Informationssicherheit definieren
- Die AGB Auslagerung Informatikleistungen in den Rahmenvertrag einbinden
- Einen Entwicklungsprozess anwenden, der die Informationssicherheit unterstützt, wie der Secure Development Life Cycle
- Die zehn häufigsten Sicherheitsrisiken für Webanwendungen des Open Web Application Project beachten (OWASP Top 10)
- Regelmässiger Code Review sowie Vier-Augen-Prinzip bei der Freigabe von kritischen Programmteilen anwenden
- Die Passwortsicherheit gewährleisten

Der Datenschutzbeauftragte wird die Kontrolle von Webhosting-Unternehmen fortführen. Von den Kontrollen und den darauf folgenden Verbesserungen bei Auftragnehmern profitieren alle Organe, die Kunden der geprüften Unternehmen sind.

Meldung einer Datenpanne

Bei einem öffentlichen Organ war nach der Migration eines Servers ein Verzeichnis von Bewerberdaten für kurze Zeit im Internet zugänglich. Der Konfigurationsfehler wurde nach der Feststellung sofort behoben.

Das öffentliche Organ meldete die Datenpanne dem Datenschutzbeauftragten mit Datum und Art des Vorfalls, Kategorien der Daten, Anzahl betroffener Personen und eingeleiteten Sofortmassnahmen. Kurz danach folgte ein ausführlicher Bericht über die Ereignisse, die Feststellungen und die getroffenen Massnahmen. Der Datenschutzbeauftragte nahm zur Kenntnis, dass die notwendigen Massnahmen getroffen worden waren und kein weiterer Handlungsbedarf bestand. Die Meldung und die Problembehebung durch das betreffende öffentliche Organ waren vorbildlich.

Das zukünftige IDG sieht für solche Vorfälle neu eine Meldepflicht an den Datenschutzbeauftragten und unter Umständen die betroffenen Personen vor (Vorlage 5471, § 12a revIDG).

SwissID für die Verwaltung

Die SwissID der Firma SwissSign löst die SuisseID der Post ab. Der kostenlose Identifikationsdienst soll zukünftig in allen Bereichen als digitale Identität genutzt werden. Die SwissID soll zur Authentisierung bei Onlinediensten, Banken und Versicherungen wie auch bei Behörden dienen. Die gesetzliche Grundlage ergibt sich aus der Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift nach Art. 14 Abs. 2bis OR.

Aktuell kann die SwissID nur bei der Post genutzt werden. Die anderen Provider und Dienste arbeiten an der Implementation der Lösung. Auch die kantonale Verwaltung möchte in Zukunft zahlreiche Dienste digital anbieten, um so den Gang auf die jeweilige Behörde entfallen lassen zu können. Dabei wird die SwissID eine wichtige Rolle spielen, wenn es um die eindeutige Identifizierung über das Internet geht. Um verschiedene, nicht kompatible Insellösungen zu vermeiden, soll die Nutzung der SwissID zentral organisiert werden.

Der Datenschutzbeauftragte verfolgt und bewertet die Projekte und Initiativen zur digitalen Verwaltung und zu den digitalen Identitätsdiensten. Er wird wenn nötig Massnahmen vorschlagen.

Weitere Themen

Ein öffentliches Organ fragt, ob die Rolle des Chief Information Security Officer (CISO) zwingend geschaffen werden muss: Eine gesetzliche Pflicht besteht nicht. Je nach Grösse des Organs ist es sinnvoll, dass seine oberste Leitung ihre Verantwortung für die Einhaltung des Datenschutzes und der Informationssicherheit an eine Person in der CISO-Rolle delegiert.

Diebstahl von Nutzerdaten bei einem grossen Telekommunikationsdienstleister, der für den Kanton Zürich tätig ist: Der Kanton erstellte in Zusammenarbeit mit dem Datenschutzbeauftragten ein Schreiben, in dem er die stark verspätete Information über den Vorfall kritisierte und unter anderem einen Zeitplan für die Umsetzung verbesserter Sicherheitsmassnahmen verlangte.

Private verlangen von kantonalen Stellen, eine Vertraulichkeitserklärung zu unterzeichnen, bevor sie Einsicht in Personendaten erteilen: Das Vorgehen ist unter privaten Stellen üblich. Für öffentliche Organe ist es nicht anwendbar, da ihre Mitarbeitenden dem Amtsgeheimnis unterstehen.

Beurteilung des Nutzungsreglements einer Schule für die Verwendung von Facebook: Die Regeln für die Nutzung sozialer Medien an Schulen sind im privatim-Merkblatt Datenschutzkonforme Nutzung sozialer Medien durch öffentliche Organe beschrieben. Die Schülerinnen und Schüler sind für die Risiken der Nutzung von sozialen Medien zu sensibilisieren.

Agile Daten

Digital unterwegs – Öffentliche Organe in der Pflicht

Öffentliche Organe haben eine besondere Verantwortung, wenn sie die Daten der Bürgerinnen und Bürger bearbeiten. Bei jedem digitalen Produkt muss überprüft werden, wie und wo die Daten bearbeitet werden, mit welchen Risiken eine solche Datenbearbeitung behaftet ist und welche Massnahmen zur Minderung der Risiken umgesetzt werden. Die Produktepalette wächst ununterbrochen. Die Abklärungen sind häufig komplex und zeitintensiv.

Datenschutzkonforme Messenger-Dienste vorhanden

Der Datenschutzbeauftragte behandelte viele Anfragen zu Messenger-Diensten, allen voran zu Whatsapp. Der Einsatz von Whatsapp in den Schulen, in der Verwaltung oder durch die Spitex ist nicht datenschutzkonform. Dabei spielen verschiedene Aspekte eine Rolle, beispielsweise die von Whatsapp festgelegte Altersgrenze auf 16 Jahre, die mögliche Verknüpfung der Daten durch Facebook oder die Übermittlung von besonderen Personendaten, beispielsweise Gesundheitsdaten. Entscheidend für die datenschutzrelevante Beurteilung ist jedoch die Tatsache, dass bei der Nutzung dieser App die Daten aller im Adressbuch erfassten Personen an Facebook übermittelt werden, auch die von nicht Whatsapp-Nutzenden. Datenschutzkonforme Alternativen sind vorhanden. Der Datenschutzbeauftragte stellt im Merkblatt Kommunikationssoftware eine Übersicht zur Verfügung.

Ein Amt wollte zur Studienberatung einen Dienst verwenden, der die Nutzung von Whatsapp voraussetzt. Werden solche anderen Dienste, beispielsweise Whatsbroadcast, in Erwägung gezogen, sind diese auch mit Blick auf die vorgelagerten Dienste, in diesem Fall Whatsapp, zu beurteilen.

Häufig beziehen sich Anfragen auch auf Kommunikations- und Zusammenarbeitsplattformen. Oft wird heute vorausgesetzt, dass alle Beteiligten jederzeit und überall einfach auf die Projektdaten zugreifen können. Eine Gemeinde fragte den Datenschutzbeauftragten, ob eine Plattform zur Vernetzung der Bürgerinnen und Bürger eingesetzt werden kann. Fragen zu Verantwortlichkeiten, zu Zugriffsregelungen und zur Umsetzung der Sicherheitsmassnahmen stehen bei diesen Plattformen im Mittelpunkt. Die Gemeinde bleibt für die Inhalte verantwortlich, auch wenn sie eine solche Plattform über einen Auftragsdatenbearbeiter zur Verfügung stellt. Bei Zusammenarbeitsplattformen sind die Zugriffsberechtigungen zu regeln. Bei einer elektronischen Bearbeitung der Personaldaten mit dem Produkt HR Informationsportal für Führungskräfte dürfen beispielsweise nicht alle Nutzenden auf alle Daten Zugriff haben. Dem Grundsatz der Verhältnismässigkeit entsprechend ist der Zugriff auf die Informationen zu beschränken, die für die jeweilige Aufgabenerfüllung notwendig sind. Bei ausländischen Produkten spielen je nach Sensitivität der Daten das anwendbare Recht und der Gerichtsstand eine zentrale Rolle.

Die Risiken des vereinfachten Datenaustauschs

Die Personendaten werden mobiler. Einmal erfasst, sollen sie immer breiter genutzt werden können. Dabei sind der Persönlichkeitsschutz und die persönliche Freiheit der betroffenen Personen sicherzustellen.

Der Datenschutzbeauftragte stellt eine zunehmende Tendenz fest, dass Personendaten zwischen öffentlichen Organen ausgetauscht werden. Zudem werden Personendaten immer häufiger veröffentlicht – insbesondere im Internet. Getrieben wird diese Entwicklung durch die neuen Technologien, die den Datenaustausch vereinfachen. Der Datenschutzbeauftragte hat im Rahmen seiner Beratungs- und Aufsichtstätigkeit darauf hingewiesen, dass die datenschutzrechtlichen Grundsätze einzuhalten sind, insbesondere der Zweckbindungsgrundsatz. Weiter ist die Informationssicherheit zu gewährleisten. Die Fragestellungen in den einzelnen Anfragen werden allerdings immer komplexer.

Vorabkontrolle der Kantonalen Einwohnerdatenplattform

Die Kantonale Einwohnerdatenplattform (KEP) soll den Austausch von Einwohnerdaten zwischen verschiedenen öffentlichen Organen des Kantons ermöglichen. Die öffentlichen Organe erhalten Zugriff auf ein Replikat der kommunalen Einwohnerregister und können elektronisch Personendaten aus Einwohnerregistern abrufen. Die KEP wird durch Mutationsmeldungen aktuell gehalten. Der Datenschutzbeauftragte begleitete dieses Vorhaben schrittweise. Er nahm Stellung im Rahmen von Vernehmlassungen zum Gesetz über das Meldewesen und die Einwohnerregister sowie zur dazugehörigen Verordnung und wies auf die Sensibilität der Datenbearbeitungen hin, unter anderem aufgrund der grossen Anzahl betroffener Personen. Weiter hat er das Projektteam im Verlauf des Projekts beraten und datenschutzrechtliche und -technische Aspekte aufgezeigt, die beachtet werden müssen. Schliesslich verlangte er die Vorlage des Projekts zur Vorabkontrolle. Sie ist noch nicht abgeschlossen.

Erweiterung der Identifikatoren und Merkmale im Einwohnerregister

Verschiedene Bürgerinnen und Bürger wandten sich an den Datenschutzbeauftragten und wiesen darauf hin, dass Gemeinden in den Einwohnerregistern eine grosse Anzahl zusätzlicher Merkmale und Identifikatoren führen. Der Datenschutzbeauftragte klärte diese Hinweise ab. Er stellte fest, dass ein Verband den Einwohnerkontrollen aufzeigte, wie die Führung der zusätzlichen Merkmale durch einen Erlass eines kommunalen Beschlusses ermöglicht werden könne. Der Datenschutzbeauftragte klärte die Rechtslage mit dem Verband und dem Gemeindeamt. Die Bearbeitung der grossen Anzahl zusätzlicher Merkmale in den Einwohnerregistern ist mit den datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Das Vorgehen verletzt die Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit, der Transparenz und der Richtigkeit. Öffentliche Organe dürfen Personendaten nur gestützt auf eine rechtliche Grundlage bearbeiten und nicht aufgrund einer Einwilligung der betroffenen Personen.

Das Gemeindeamt und der Datenschutzbeauftragte kamen zum Schluss, dass gemeinsame Kontrollen bei den Einwohnerkontrollen durchzuführen sind. Zudem soll die Verordnung über das Meldewesen und die Einwohnerregister mit weiteren Datenkategorien ergänzt werden. Der Datenschutzbeauftragte wird im Rahmen der Vernehmlassung die Einhaltung der datenschutzrechtlichen Grundsätze prüfen.

Einbürgerungsentscheide auf der Website

Eine Gemeinde wandte sich mit der Frage an den Datenschutzbeauftragten, ob die auf der Website publizierten Sitzungsprotokolle des Gemeinderats zu löschen sind, die Einbürgerungsentscheide enthalten. Anlass der Anfrage war ein Gesuch einer im Jahr 2008 eingebürgerten Person um Löschung der sie betreffenden Daten. Der Datenschutzbeauftragte hielt zunächst fest, dass die Publikation von Personendaten im Internet auf einer gesetzlichen Grundlage beruhen und verhältnismässig sein muss. Aus der Verhandlungsöffentlichkeit des Gemeinderats kann auch die Publikation der Gemeinderatsprotokolle abgeleitet werden.

Aufgrund einer neuen Regelung in der Kantonalen Bürgerrechtsverordnung aus dem Jahr 2018 sind die Daten zu den Einbürgerungsgeschäften nach Eintritt der Rechtskraft des Einbürgerungsentscheids aus dem Protokoll zu löschen. Jedoch war auch vor Inkrafttreten dieser neuen Regelung der Grundsatz der Verhältnismässigkeit zu beachten. Deshalb ist zwischen dem Interesse, die Öffentlichkeit über erfolgte Einbürgerungen zu informieren, und dem Interesse der eingebürgerten Person am Schutz ihrer Privatsphäre abzuwägen. Diese Beurteilung verändert sich im Lauf der Zeit: Das Interesse der Öffentlichkeit an der Information nimmt ab, wodurch das Interesse der betroffenen Personen am Schutz ihrer Privatsphäre stärker zu gewichten ist. Damit sind Informationen über Einbürgerungswillige im Internet zu löschen, sobald der Zweck der Veröffentlichung erfüllt ist. Entsprechend sind die Abschnitte aus den im Internet publizierten Gemeinderatsprotokollen zu löschen, die Einbürgerungsgeschäfte betreffen.

Publikation von Baugesuchen im Internet

Bei einer Gemeinde stellte sich die Frage, ob die Publikation von Baugesuchen auf der Website zulässig ist. Sie berief sich auf das Öffentlichkeitsprinzip. Der Datenschutzbeauftragte wies darauf hin, dass die Publikation von Gemeinderatsbeschlüssen über erteilte Baubewilligungen einer gesetzlichen Grundlage bedarf und verhältnismässig sein muss. Das Öffentlichkeitsprinzip ist als Rechtsgrundlage für die Publikation von baurechtlichen Entscheiden nicht ausreichend. Der Datenschutzbeauftragte hat der Gemeinde daher geraten, auf die Publikation zu verzichten.

Der baurechtliche Entscheid wird im Rahmen eines formellen Verfahrens gefällt. Der Umgang mit Informationen dazu richtet sich deshalb nach dem Verfahrensrecht. Jede Person, die Ansprüche geltend machen will, hat das Recht, die Zustellung des baurechtlichen Entscheids innert einer bestimmten Frist zu verlangen. Dadurch wird die Öffentlichkeit der Entscheide gewahrt. Über erteilte Baubewilligungen kann im amtlichen Publikationsorgan wie auch auf der Website in kurzer Form und in verhältnismässigem Umfang informiert werden, wenn der baurechtliche Entscheid rechtskräftig ist. Dies liegt im Ermessen der Gemeinde. Die Publikationsdauer ist zeitlich zu beschränken oder die Indexierung durch Suchmaschinen zu verhindern.

Eine Person beschwerte sich bei einer Gemeinde darüber, dass ihre Adresse aufgrund der im Internet publizierten Baubewilligung ersichtlich ist. Für die Adresse bestand eine Datensperre. Der Datenschutzbeauftragte hat der Gemeinde mitgeteilt, dass die Information über Baubewilligungen in verhältnismässiger Weise erfolgen muss. Das Bauprojekt sei aufgrund der Publikation gemäss Planungs- und Baurecht bereits bekannt. Personendaten dürfen aber nur so lange publiziert werden, wie der Zweck der Publikation dies erfordere. Dies könne durch eine zeitliche Beschränkung wie auch eine Verhinderung der Indexierung durch Suchmaschinen erreicht werden. Eine Datensperre im Einwohnerregister hat keinen Einfluss auf diese Publikation.

Datensammeln mit digitalen Stromzählern einschränken

Ein Energieversorger einer Gemeinde wandte sich an den Datenschutzbeauftragten, weil er für die Umsetzung der Energiestrategie 2050 digitale Stromzähler, so genannte Smart Meter, installieren wollte. Der Datenschutzbeauftragte stellte fest, dass für den Einsatz von digitalen Stromzählern eine Rechtsgrundlage besteht. Weiter wies er auf die datenschutzrechtlichen Grundsätze hin. Gestützt auf den Verhältnismässigkeitsgrundsatz dürften nur jene Personendaten erhoben werden, die für die Aufgabe, etwa die Rechnungsstellung, notwendig sind. Zudem sind die Zugriffsberechtigungen auf die Personendaten zu regeln, beispielsweise mit einem Rollenkonzept. Die Personendaten dürfen zudem nur zu dem Zweck bearbeitet werden, zu dem sie erhoben worden sind. Die Bearbeitung der Personendaten zu einem anderen Zweck bedarf einer Rechtsgrundlage oder der Einwilligung der betroffenen Person. Schliesslich ist mit geeigneten organisatorisch-technischen Massnahmen zur Informationssicherheit sicherzustellen, dass die Vertraulichkeit, die Integrität und die Verfügbarkeit der Personendaten gewährleistet sind. Dafür eignet sich zum Beispiel die Verschlüsselung der Personendaten bei der Speicherung wie auch bei der Übermittlung.

Grenzenlose Datenflüsse

Daten machen an den Schweizer Grenzen nicht halt. Im öffentlichen Bereich trifft dies vor allem zu auf Auftragsdatenbearbeitungen oder auf Strafverfolgungsorgane, die international zusammenarbeiten. Die Schweiz ist Teil des Schengen-Raums und muss die geltenden Rahmenbedingungen erfüllen.

Das schweizerische Datenschutzrecht bietet den Betroffenen bei Datenbearbeitungen einen bestimmten Schutz. Das öffentliche Organ muss sicherstellen, dass dieser Schutz auch gewährleistet ist, wenn die Datenbearbeitungen ins Ausland ausgelagert werden. Es kann beispielsweise mit Verträgen die Rechte und Pflichten der Auftragsdatenbearbeiter detailliert regeln und verlangen, dass Massnahmen zum Schutz der Daten umgesetzt werden. Dies gilt besonders für Cloud-Dienstleistungen, deren Nutzung zunehmend zur Norm wird.

Auch müssen die schweizerischen Gesetze den europäischen Standard aufnehmen und umsetzen, wie derzeit mit der Revision des IDG oder des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich.

Der Datenschutzbeauftragte beurteilt regelmässig Schengen-relevante Entwicklungen im Gesetzgebungsbereich. Er prüft europäische Erlasse und nimmt Stellung zu Änderungen in eidgenössischen und kantonalen Gesetzen, beispielsweise zur Übernahme und Umsetzung von drei EU-Verordnungen zum Schengener Informationssystem (SIS).

Er behandelte viele Anfragen zu den Auswirkungen der DSGVO auf öffentliche Organe. Die extraterritoriale Wirkung der DSGVO, also ihre Wirkung ausserhalb von EU-Ländern, greift nur in wenigen Fällen. Für die öffentlichen Organe bestand meistens kein Handlungsbedarf.

Persönliche Freiheit

Anpassungen des IDG und Strategie Digitale Verwaltung

Im Jahr 2018 hat der Regierungsrat die Revision des Informations- und Datenschutzgesetzes (IDG) zuhanden des Kantonsrats verabschiedet. Er beschränkte sich dabei auf Anpassungen, die im Rahmen der Schengen-Assoziierung der Schweiz sowohl auf Bundes- wie auch auf Kantonsebene notwendig wurden. Auch 2018 hat der Regierungsrat die Strategie Digitale Verwaltung 2018–2023 beschlossen. Sie soll die Art und Weise der Datenbearbeitungen und die Zusammenarbeit der öffentlichen Organe grundlegend verändern. Erst in einem späteren Schritt sollen diesbezügliche Anpassungen des IDG erfolgen.

Der Regierungsrat hat sich bei der Revision des IDG auf die Wegleitung der Konferenz der Kantonsregierungen (KdK) gestützt, die den Kantonen als Grundlage für die Anpassung der Gesetzgebung an die EU-Richtlinie im Bereich Polizei und Justiz dient. Das Schengen-Assoziierungsabkommen der Schweiz mit der EU verpflichtet den Bund und die Kantone, die Richtlinie umzusetzen. Die EU evaluiert regelmässig die Zusammenarbeit im Rahmen des Schengen-Abkommens. Dabei wird auch die Umsetzung des Datenschutzes beurteilt (Seite 8). Der Datenschutzbeauftragte nahm im Rahmen der Vernehmlassung zum Gesetzesprojekt Stellung. Generell konnte der Datenschutzbeauftragte feststellen, dass die Anforderungen des KdK-Leitfadens gut aufgenommen und pragmatisch umgesetzt wurden. Seine Bemerkungen bezogen sich auf einige zu klärende Ergänzungen.

Offene Punkte der Umsetzung

In der Weisung an den Kantonsrat vom 4. Juli 2018 (KR Nr. 5471) wurden allerdings materielle Änderungen vorgenommen, die nicht konform zu den Vorgaben der Richtlinie sind. In der Vorlage fehlt die verpflichtende Bestimmung, dass sich ein Bürger oder eine Bürgerin mit einer Beschwerde an den Datenschutzbeauftragten wenden kann, mit der sich dieser in einem förmlichen Verfahren zu befassen hat. Im Schengen-Datenschutzgesetz (SDSG) des Bundes wird diese Vorgabe gelöst, indem die Möglichkeit einer Anzeige beim Datenschutzbeauftragten mit folgender Verpflichtung festgeschrieben ist: «Hat die betroffene Person Anzeige erstattet, so informiert der Beauftragte sie über die gestützt darauf unternommenen Schritte und das Ergebnis einer allfälligen Untersuchung.» Dieses Recht muss auch der Zürcher Bevölkerung gewährt werden.

Weiter wird die Hürde für die Ausübung der Aufsicht des Datenschutzbeauftragten erhöht: Eine Verfügung zur Anpassung der Datenbearbeitungen soll nur bei einer «erheblichen» Verletzung von Bestimmungen über den Datenschutz möglich sein. «Erheblich» ist aber ein unbestimmter Rechtsbegriff und es ist nicht sinnvoll, wenn im Vorfeld einer Verfügung darüber gestritten wird, was «erheblich» ist. Das Gebot der Verhältnismässigkeit gilt in jedem Fall. Bei einer nicht erheblichen Verletzung von Bestimmungen wäre eine Verfügung des Datenschutzbeauftragten entsprechend unverhältnismässig.

Gestrichen wurde zudem die Möglichkeit, dass der Datenschutzbeauftragte vorsorgliche Massnahmen erlassen kann. Die gestrichene Formulierung lautete: «Die oder der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete schutzwürdige Interessen zu schützen oder Beweismittel zu sichern.»

Dies sind drei wichtige Bestimmungen, um die Freiheitsrechte der Bürgerinnen und Bürger angesichts der umfassenden Digitalisierung zu schützen und bei Datenschutzproblemen effizient und effektiv eingreifen zu können. Der Datenschutzbeauftragte wurde von der zuständigen Kommission (StGK) zu einer Anhörung eingeladen, in der er diese Punkte konkretisieren konnte. Ende 2018 war die Gesetzesrevision noch bei der Kommission anhängig.

Digitalisierung ohne Datenschutz?

Der Datenschutzbeauftragte hatte die Gelegenheit, vor der Verabschiedung der Strategie Digitale Verwaltung 2018–2023 Stellung zu beziehen. Die Digitalisierung der Verwaltungsabläufe beinhaltet unzählige Interaktionen mit internen und externen Personen und Organisationen. Dies führt zu einem exponentiellen Anwachsen der Datenmenge bei der Verwaltung, da jede digitale Interaktion Datenspuren hinterlässt. So wird zwangsläufig festgehalten, wer wann mit wem und wie oft welche Informationen und Daten ausgetauscht hat. Die zahlreichen Schnittstellen, die sich aus der Interaktion mit der Verwaltung ergeben, beispielsweise bei der Nutzung des Smartphones, führen aber immer auch dazu, dass private Datenbearbeiter über diese Interaktionen Daten erhalten (Hard- und Softwarehersteller, Telekomanbieter etc.).

Die Aufbewahrung, Bearbeitung oder Auswertung von Datenspuren ermöglicht die Erstellung von Profilen der betroffenen Personen. Dies ist oft Teil der Geschäftsmodelle im Privatbereich. Es kann nicht davon ausgegangen werden, dass die betroffenen Personen, die sich im Privatbereich ständig mit der Auswertung ihrer Verhaltensspuren konfrontiert sehen, die Auswertung solcher Daten auch von der staatlichen Verwaltung akzeptieren. Im Gegenteil: Der Staat hat ihre Grundrechte zu wahren. Die Verwaltung muss deshalb dafür sorgen, dass diesen Auswertungen nicht Vorschub geleistet wird, und muss ausschliessen, dass die Überwachung von Mitarbeitenden oder die Erstellung von Verhaltensprofilen von Bürgerinnen und Bürger ermöglicht wird. Deshalb sollen für die Interaktion datenschutzfreundliche Produkte gewählt werden. Der richtige und sichere Umgang mit den Daten ist kritisch für die Akzeptanz und das Vertrauen der betroffenen Personen. Wie diesen Herausforderungen der Digitalisierung begegnet wird, bleibt mit der vorliegenden Strategie weitgehend offen. Dafür bräuchte es eine Politik der Datenvermeidung und der Datensparsamkeit als Teil der Strategie der Digitalisierung. Der Datenschutzbeauftragte schlug deshalb vor, dass das Leitbild mit einem übergeordneten Zweck ergänzt wird, der mit der Digitalisierung im Kanton Zürich erreicht werden soll. Darin müsste zum Ausdruck kommen, dass die Digitalisierung zur Stärkung des Rechtsstaats und seiner Institutionen, der föderalen Demokratie und der Grundrechte beitragen soll. Zudem wurde der Datenschutzbeauftragte in der Organisationsstruktur zur Umsetzung der Digitalisierung der Verwaltung in keiner Art und Weise einge-bunden. Dies erachtet der Datenschutzbeauftragte als einen schwerwiegenden Mangel, da die Fragen des Schutzes und der Sicherheit der Daten bei der Digitalisierung eine zentrale Rolle spielen müssen.

Pragmatische Zusammenarbeit

Die Anmerkungen des Datenschutzbeauftragten wurden nicht in die Strategie aufgenommen. Der Datenschutzbeauftragte versuchte deshalb, die Zusammenarbeit mit den direkt involvierten Stellen zu intensivieren. Bis Ende 2018 ist es gelungen, in verschiedenen Bereichen eine Zusammenarbeit auf einer pragmatischen Grundlage zu etablieren. Auch bei den betroffenen öffentlichen Organen stand die Erkenntnis im Vordergrund, dass ohne eine angemessene Berücksichtigung der Anliegen des Datenschutzes digitale Lösungen in der Bevölkerung kaum akzeptiert werden (Seite 7).

Einschränkungen der persönlichen Freiheit

Der Datenschutzbeauftragte nahm Stellung zu verschiedenen Gesetzes- und Verordnungsvorlagen, in denen Fragen zur Einschränkung oder Gefährdung der persönlichen Freiheit zentral waren.

Totalrevision des Sozialhilfegesetzes

Der Datenschutzbeauftragte beurteilte in seiner Stellungnahme die Regelungen der Datenbearbeitungen im Entwurf des totalrevidierten Sozialhilfegesetzes als gelungen. Er begrüsste, dass die Bestimmungen zum Informationsaustausch bestehen bleiben (Schweigepflicht, Informationsaustausch, Amtshilfe). Das revidierte Gesetz erfüllt damit die Voraussetzungen für Grundrechtseinschränkungen sowie die Anforderungen an Rechtsgrundlagen für Datenbekanntgaben.

Der Gesetzesentwurf beinhaltet eine Regelung, die bei einem Wechsel des Unterstützungswohnsitzes als Rechtsgrundlage dienen soll für die sofortige Übergabe des vollständigen Sozialhilfedossiers an das neu zuständige Sozialhilfeorgan. Der Datenschutzbeauftragte forderte die Streichung dieser Regelung und zeigte die Rechtslage auf. Als öffentliches Organ unterliegt die Sozialhilfebehörde einer Dokumentations- und Aufbewahrungspflicht. Deshalb darf sie die Unterlagen nicht an ein anderes Organ übergeben. Die Übergabe des vollständigen Sozialhilfedossiers wäre zudem unverhältnismässig. Der verhältnismässige Informationsfluss ist bereits mit den bestehenden rechtlichen Bestimmungen gewährleistet.

Weiter nahm er Stellung zur neuen Bestimmung zur Observation. Er stellte fest, dass eine Observation einen schweren Eingriff in das Grundrecht auf Privatsphäre darstelle. Deshalb begrüsste er den Erlass einer formell-gesetzlichen Regelung für den Einsatz von Sozialdetektivinnen und Sozialdetektiven wie auch die Umsetzung der Rahmenbedingungen einer Observation gemäss dem Urteil des Europäischen Gerichtshof für Menschenrechte vom 18. Oktober 2016 zum Fall Vukota-Bojic gegen die Schweiz. Er wies darauf hin, dass auch für Hausbesuche im Sozialhilfebereich eine ausdrückliche Rechtsgrundlage zu schaffen ist, falls diese Massnahme weiterhin eingesetzt werden soll. Mit Hausbesuchen werde zusätzlich das Grundrecht auf Schutz der Wohnung tangiert.

Änderung der Verordnung über den allgemeinen Teil des Sozialversicherungsrechts

Der Datenschutzbeauftragte begrüsste in seiner Stellungnahme zur Änderung der Verordnung über den allgemeinen Teil des Sozialversicherungsrechts, dass für Observationen eine Bewilligungspflicht vorgesehen ist und die fachlichen und persönlichen Anforderungen an die Personen definiert werden, die im Auftrag von Versicherungsträgern Observationen durchführen dürfen. Weiter begrüsste er, dass das Verfahren zur Einsichtnahme in das vollständige Observationsmaterial geregelt wird. Zu den Bestimmungen zu Aktenführung und Aktenaufbewahrung hielt er fest, dass diese nicht auf die Versicherungsträger zu beschränken sind. Auch für die beauftragten Spezialistinnen und Spezialisten sei zu regeln, wie sie die Akten zu führen sowie das Observationsmaterial aufzubewahren haben und die Einhaltung des Datenschutzes und der Datensicherheit gewährleisten müssen. Observationsmaterial, das nicht auf unrechtmässigen Leistungsbezug schliessen lässt, sei nach Erlass der Verfügung zu vernichten. Zudem müssten die von Versicherungsträgern mit Observationen beauftragten Personen das Observationsmaterial nach Beendigung des Auftrags dem Versicherungsträger übergeben.

Systematische Verwendung der AHV-Nummer

Der Datenschutzbeauftragte nahm Stellung zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHV) zur systematischen Verwendung der AHV-Nummer durch Bundesbehörden. Er stellte fest, dass die Vorlage die Risiken für die Persönlichkeitsrechte der Bürgerinnen und Bürger erhöht. Im Rahmen der Digitalisierungsvorhaben der Verwaltung müsse für die Verwendung der AHV-Nummer eine klare Ausgangslage geschaffen werden, welche die rechtlichen, organisatorischen und technischen Aspekte gleichermassen berücksichtige. Der Datenschutzbeauftragte kritisierte, dass das Sicherheitskonzept für Personenidentifikatoren der Kommission für Rechtsfragen des Nationalrates nicht abgewartet wurde. Im Konzept, das aufgrund des Postulats 17.3968 in Auftrag gegeben worden war, soll definiert werden, wie bei der Verwendung der AHV-Nummer den Risiken für den Datenschutz und die Sicherheit begegnet werden kann. Das Vorziehen der Gesetzesänderung führe zur unbefriedigenden Situation, dass die Kantone eigenständig Risikoanalysen durchführen und prüfen müssten, ob die AHV-Nummer oder ein bereichsspezifischer Identifikator einzusetzen ist. Für die Schaffung eines einheitlichen eidgenössischen Personenidentifikators fehle zudem die verfassungsrechtliche Grundlage. Deshalb sei klarer auszuführen, dass die systematische Verwendung der AHV-Nummer nicht die Schaffung eines einheitlichen eidgenössischen Personenidentifikators bedeute. Aus datenschutzrechtlicher Sicht ist die Verwendung verschiedener, sektorieller Personenidentifikatoren zu bevorzugen, da die rechtlichen und technischen Risiken eines universellen Identifikators zu hoch sind.

Der Datenschutzbeauftragte stellte infrage, ob überhaupt ein genügender Regulierungsbedarf besteht. Einerseits werde die systematische Verwendung der AHV-Nummer angestrebt, um die korrekte Verknüpfbarkeit von Datenbanken zu erhöhen. Andererseits sei dem Bericht zur Vorlage zu entnehmen, dass die Zuverlässigkeit der Verknüpfbarkeit auch ohne Verwendung der AHV-Nummer bei 99,98 Prozent liege. Dem finanziellen und administrativen Aufwand stehe kein entsprechender Nutzen gegenüber.

Kontakt

E-Mail	datenschutz@dsb.zh.ch
Adresse	Datenschutzbeauftragter des Kantons Zürich, Postfach, CH-8090 Zürich
Internet	www.datenschutz.ch
Twitter	twitter.com/dsb_zh
Youtube	www.youtube.com/channel/UCghVVLU_hOTbClYaKQk8hTw
Telefon	+41 43 259 39 99

Impressum

Herausgeber	Datenschutzbeauftragter des Kantons Zürich, Postfach, 8090 Zürich
Korrektorat	Text Control, Im Struppen 11, 8048 Zürich
Grafik	TKF Kommunikation & Design, t-k-f.ch

Der Tätigkeitsbericht 2018 ist elektronisch verfügbar unter
www.datenschutz.ch/tb2018.

ISSN 2571-5003

Datenschutz mit Qualität

datenschutz.ch