dsb

datenschutzbeauftragter
kanton zürich

2013

Tätigkeitsbericht

Datenschutzbeauftragter Kanton Zürich

- Der Datenschutzbeauftragte 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 (Datenschutz-Reviews), 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.

«Im Zeitalter des Internets der Dinge wird Medienkompetenz immer wichtiger.»

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 2013 bis und mit 31. Dezember 2013 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, März 2014

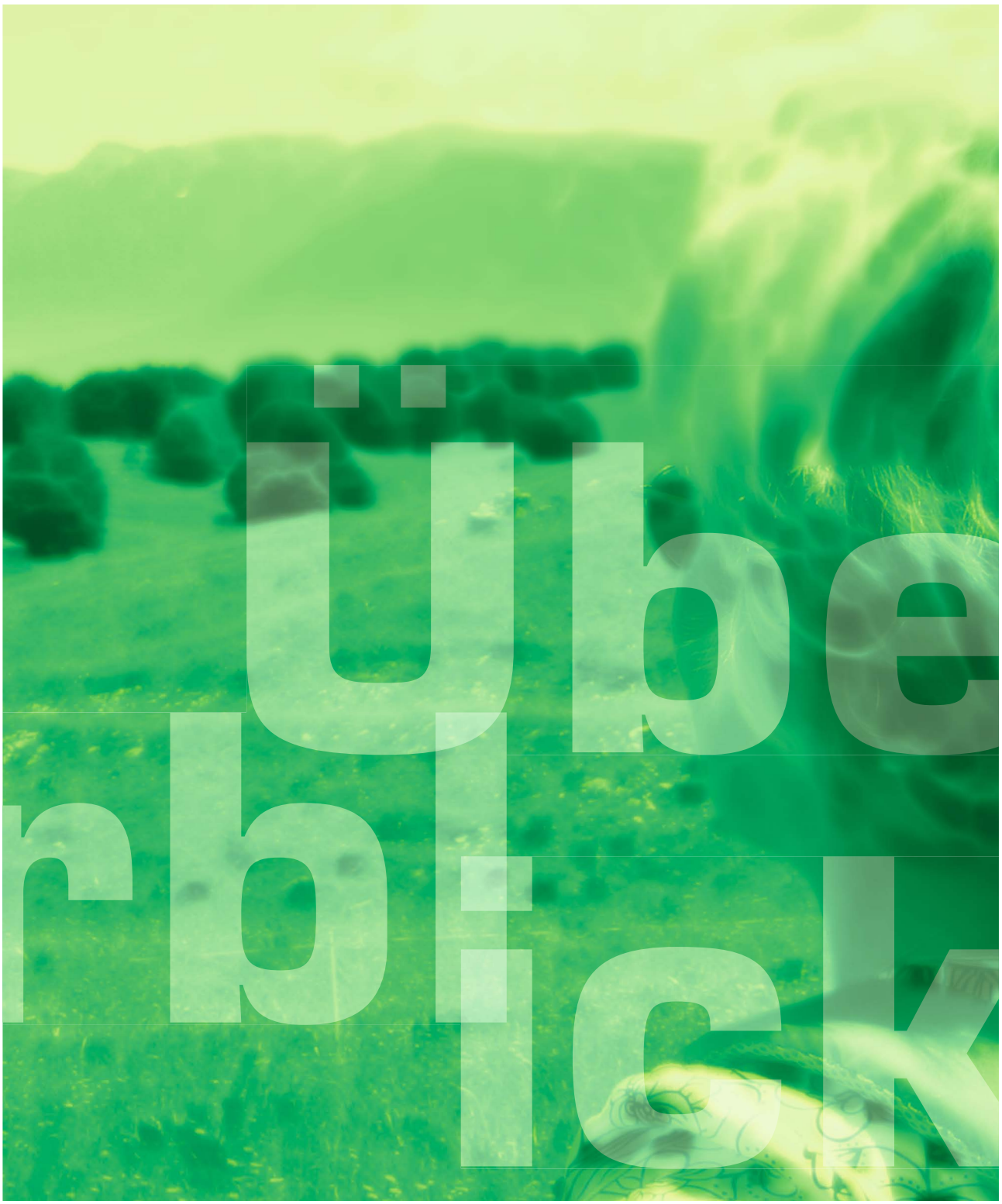
Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Überblick

Beratung

Vernehmlassungen

Kontrollen & Vorabkontrollen



überblick

«Datenlecks und Enthüllungen haben vielen Menschen erst bewusst gemacht, welchen Risiken ihre persönlichen Daten ausgesetzt sind.»

Wo sind meine Daten?

Immer mehr Bürgerinnen und Bürger wollen wissen, was mit ihren persönlichen Daten geschieht. Sie sind besorgt, dass ihre Daten missbraucht werden könnten. Dies schlägt sich auch in der Beratungstätigkeit des Datenschutzbeauftragten nieder.

Die Medien berichteten im vergangenen Jahr ausführlich über Datenlecks in Unternehmen und Verwaltung, und die Enthüllungen von Edward Snowden zu den Praktiken der amerikanischen National Security Agency zeigten auf, wie flächendeckend die digitale Kommunikation überwacht wird und die Daten ausgewertet werden können. Vielen Personen ist erst dadurch bewusst geworden, welchen Risiken ihre persönlichen Daten ausgesetzt sind.

Klarheit über Datenbearbeitungen

Es erstaunt deshalb nicht, dass auch Bürgerinnen und Bürger im Kanton Zürich sich vermehrt Sorgen machen und sich die Frage stellen, ob ihre Daten bei den öffentlichen Organen wirklich geschützt sind. Dies hat sich auch in einer spürbaren Zunahme der Anfragen beim Datenschutzbeauftragten geäussert. Die betroffenen Personen wollten Klarheit darüber, welche Daten über sie bearbeitet werden, aber auch Gewissheit, dass diese vor Missbrauch geschützt sind.

Der Datenschutzbeauftragte konnte dabei auf das Auskunftsrecht verweisen, das jeder Person das Recht gibt, bei einem öffentlichen Organ Auskunft darüber zu verlangen, welche Daten über sie bearbeitet werden. Bei überwiegenden öffentlichen oder privaten Interessen kann die Auskunft eingeschränkt werden. Diese Einschränkung muss vom öffentlichen Organ allerdings begründet und mittels Verfügung mitgeteilt werden. In zahlreichen Fällen hatte der Datenschutzbeauftragte sowohl der betroffenen Person wie auch dem öffentlichen Organ das Vorgehen zu erläutern oder er vermittelte diesbezüglich zwischen den Parteien.

Zur Transparenz über die Datenbearbeitungen trägt aber auch eine klare Gesetzgebung bei. Insbesondere das Bearbeiten von sensitiven Personendaten durch die öffentlichen Organe ist ein deutlicher Eingriff in die Persönlichkeitsrechte und das Grundrecht auf persönliche Freiheit. Das Informations- und Datenschutzgesetz (IDG) verlangt deshalb eine hinreichend bestimmte Regelung in einem formellen Gesetz. Damit erhalten die betroffenen Personen Klarheit darüber, welche Organe welche persönlichen Daten über sie erheben, austauschen und aufbewahren. Diese Transparenz schafft Vertrauen in die Datenbearbeitung der öffentlichen Organe. Auch der Gesetzgeber sollte dies bedenken und generalklauselartige Bestimmungen diesbezüglich hinterfragen.

Kontrollen schützen vor Missbrauch

Gewissheit darüber zu erlangen, dass die persönlichen Daten nicht missbraucht werden können, ist schwierig. Voraussetzung hierfür ist, dass die öffentlichen Organe alle angemessenen Massnahmen ge-

troffen haben, um die Daten zu schützen. Nur dadurch kann das – nicht vermeidbare – Restrisiko eines Datenmissbrauchs auf ein Minimum beschränkt werden. Der Datenschutzbeauftragte kontrolliert diesbezüglich die öffentlichen Organe. Im Rahmen einer standardisierten «Datenschutz-Review» wird geprüft, ob die Grundschutzmassnahmen im organisatorischen und im technischen Bereich getroffen worden sind. Zusätzlich werden auch die rechtlichen Voraussetzungen der Datenbearbeitung fallweise geprüft. Bestimmte Datenbearbeitungen in sensitiven Bereichen werden einer vertieften Prüfung unterzogen. Die Ergebnisse der Prüfung münden in Hinweise an die öffentlichen Organe, wie sie die Sicherheit ihrer Datenbearbeitung besser gewährleisten können. Leider zeigen die Ergebnisse der Prüfungen, dass im Durchschnitt nur zwischen einem und zwei Dritteln der erforderlichen Massnahmen für einen Grundschutz der Daten getroffen sind. Mit anderen Worten: Die Daten sind einem nicht unbedeutenden Missbrauchsrisiko ausgesetzt.

Der Datenschutzbeauftragte trägt mit seinen Kontrollen zur Sensibilisierung in Bezug auf die Risiken bei und bietet umfangreiche Handlungsanleitungen, wie der Schutz der Daten effizient und wirksam erhöht werden kann. Das Intervall von mehr als fünf Jahren zwischen den Kontrollen bei einem einzelnen Organ ist angesichts der technologischen Entwicklung allerdings wenig nachhaltig. Eine Verbesserung der Ressourcen beim Datenschutzbeauftragten wäre wünschbar.

1993: Ja zum Datenschutz

Vor zwanzig Jahren, am 6. Juni 1993, hat die Zürcher Stimmbevölkerung mit grosser Mehrheit Ja gesagt zum ersten Datenschutzgesetz im Kanton Zürich. Damit war der Auftrag an die öffentlichen Organe klar: Die Bürgerinnen und Bürger wollen, dass ihre persönlichen Daten geschützt werden. Auch mit dem nun geltenden Informations- und Datenschutzgesetz (IDG) ist das Anliegen dasselbe geblieben. Der Datenschutzbeauftragte ist diesem gesetzlichen Auftrag verpflichtet. Seine Beratungsdienstleistungen, die Kontroll- und die Informationstätigkeit sollen dazu beitragen, die persönliche Freiheit der Bürgerinnen und Bürger zu wahren und dem Schutz der Privatsphäre den notwendigen Platz einzuräumen. Der Datenschutzbeauftragte setzt dabei auf Effizienz und Effektivität, was in einem Qualitätsmanagementsystem zusammengefasst ist, das seit zehn Jahren nach ISO 9001 zertifiziert ist. Das Qualitätsmanagementsystem unterstützt die Aufgabenerfüllung des Datenschutzbeauftragten und trägt dazu bei, die Beratungs-, Kontroll-, Vernehmlassungs-, Informations- sowie Aus- und Weiterbildungstätigkeiten kunden- und wirkungsorientiert auszurichten. Die vielen positiven Feedbacks von öffentlichen Organen und Bürgerinnen und Bürger auch im vergangenen Jahr sind erfreulich.

Weitere Schwerpunkte

- Praktische Fragen des Kindes- und Erwachsenenschutzrechts
- Neue Regeln zur Herausgabe der Patientendokumentation
- Kontrolle des Schengener Informationssystems (SIS)

Klare Bedingungen für Auslagerungen an Dritte

Die Auslagerung von Datenbearbeitungen an Dritte nimmt stark zu. Um den datenschutzrechtlichen Anforderungen an eine solche Auslagerung zu genügen, bedarf es sorgfältiger Abklärungen, eines detaillierten schriftlichen Vertrags und einer regelmässigen Überprüfung der Einhaltung der Vertragsbedingungen.

In allen Bereichen der Verwaltungstätigkeit werden Datenbearbeitungen an Dritte ausgelagert. Sie reichen vom Hosting einer Datenbank bis hin zu Aufträgen zur Durchführung von Erstgesprächen mit Migranten. Das öffentliche Organ muss sich insbesondere darüber im Klaren sein, dass es auch nach einer Auslagerung die Verantwortung für die Datenbearbeitung trägt.

Fünf Schritte zu einer datenschutzkonformen Auslagerung

Als Erstes muss geklärt werden, ob rechtliche oder vertragliche Bestimmungen einer Auslagerung entgegenstehen. Zu denken ist hier insbesondere an Berufsgeheimnisse oder andere spezielle Geheimhaltungspflichten. Wenn ja, können spezielle Schutzmassnahmen wie die Verschlüsselung von Personendaten Abhilfe schaffen.

Zweitens muss das öffentliche Organ prüfen, ob die Daten «auslagerungstauglich» sind. Dabei geht es um die Einschätzung des Gefährdungspotenzials der Daten in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität. Daten dürfen nicht unberechtigten Dritten zugänglich sein, verloren gehen oder unbefugt abgeändert werden können. Das öffentliche Organ hat diesbezüglich eine Risikoanalyse durchzuführen. Je sensitiver die Daten, desto umfassender müssen die organisatorischen, technischen und rechtlichen Massnahmen zu ihrem Schutz sein.

An dritter Stelle steht die Auswahl des Auftragnehmers. Er hat darzulegen, welche organisatorischen, technischen und rechtlichen Massnahmen zum Schutz der Daten eingesetzt werden. Insbesondere bei Standardprodukten ist es häufig so, dass keine individuellen Verträge abgeschlossen werden können und die Nutzungsbedingungen die datenschutzrechtlichen Anforderungen nicht erfüllen. Bei der Auswahl des Anbieters können Zertifikate oder Auditberichte von unabhängigen Stellen behilflich sein.

Viertens bedarf es grundsätzlich eines schriftlichen Vertrags betreffend die Auslagerung der Datenbearbeitung. Dem Erfordernis der Schriftlichkeit kann auch das Akzeptieren von Nutzungsbedingungen Genüge tun, falls diese die rechtlichen Anforderungen erfüllen und vom Anbieter nicht einseitig abgeändert werden können. Der Vertrag hat die in § 6 IDG in Verbindung mit § 25 IDV aufgeführten minimalen Anforderungen zu enthalten. Geregelt werden müssen insbesondere Gegenstand und Umfang der übertragenen Aufga-

ben, die Verantwortung, die Verfügungsmacht, die Zweckbindung, der Umgang mit Personendaten, Geheimhaltungsverpflichtungen, die Kontrollmöglichkeit des öffentlichen Organs oder einer externen Prüfstelle, die Rechte der Betroffenen, die zum Schutz der Informationen vorzukehrenden Massnahmen, die Unterauftragsverhältnisse, der Ort der Datenbearbeitung, das anwendbare Recht, der Gerichtsstand, Sanktionen bei einer Pflichtverletzung, die Vertragsdauer und die Voraussetzungen der Vertragsauflösung.

Werden besondere Personendaten ausgelagert, ist es darüber hinaus erforderlich, dass die vorgesetzte Stelle die Auslagerung der Datenbearbeitung genehmigt. Bei Auslagerungen in eine Cloud ist überdies den Clouds inhärenten Risiken wie Kontrollverlust des öffentlichen Organs und mangelnde Transparenz auf Seite der Auftragnehmenden Rechnung zu tragen.

Um die Vertragsgestaltung zu vereinfachen, hat der Datenschutzbeauftragte die «Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen» und die AGB bei einer Datenbearbeitung durch Dritte respektive bei der Inanspruchnahme externer Dienstleistungen erarbeitet. Diese können vom öffentlichen Organ bei jeder Auslagerung als integraler Bestandteil in ein Vertragsverhältnis aufgenommen werden.

Der fünfte und letzte Schritt betrifft die Kontrolle der Umsetzung der im Vertrag festgelegten Massnahmen. Es gilt, die Datenbearbeitung durch den Auftragnehmer regelmässig zu überprüfen. Zu beachten ist in diesem Zusammenhang auch die Befugnis zur Kontrolle der Datenbearbeitung durch unabhängige Organe, wie zum Beispiel den Datenschutzbeauftragten. Er ist berechtigt, sowohl bei den öffentlichen Organen wie auch bei mit der Datenbearbeitung beauftragten Dritten Kontrollen durchzuführen.

§ 6 IDG
§ 7 IDG
§ 35 IDG
§ 40 IDG
§ 25 IDV

Praktische Fragen des Kindes- und Erwachsenenschutzrechts

Per 1. Januar 2013 ist das revidierte Kindes- und Erwachsenenschutzrecht in Kraft getreten. Ergänzend dazu hat der Kanton Zürich das Einführungsgesetz zum Kindes- und Erwachsenenschutzrecht erlassen. Es zeigte sich, dass bei der Auslegung der datenschutzrechtlichen Bestimmungen zahlreiche Fragen auftauchen. Dabei ging es namentlich um die Schweigepflicht und die Amtshilfe.

Die neuen Bestimmungen des Kindes- und Erwachsenenschutzrechts haben das bisherige Vormundschaftsrecht abgelöst. Obwohl im Schweizerischen Zivilgesetzbuch (ZGB) einheitlich und übersichtlich strukturiert, finden sich auch in anderen Erlassen wie zum Beispiel im Opferhilfe- und Sozialhilfegesetz Bestimmungen zum Kindes- und Erwachsenenschutz. Bei der Umsetzung in der Praxis stellen sich Fragen zur Auslegung der datenschutzrechtlichen Bestimmungen. Dabei geht es insbesondere um die gesetzlich verankerte Schweigepflicht, die Amtshilfe sowie die Bestimmungen zur Datenbekanntgabe durch die Kindes- und Erwachsenenschutzbehörde (KESB).

Schweigepflicht verstärkt

Seit der Revision ist die Schweigepflicht explizit in Art. 451 Abs. 1 ZGB statuiert. Die vertrauliche Zusammenarbeit mit betroffenen Personen ist Voraussetzung für eine wirksame Hilfe im Bereich des Kindes- und Erwachsenenschutzes und kann nur entstehen, wenn die Betroffenen sicher sein können, dass ihre Daten vertraulich behandelt werden. Die Schweigepflicht gilt für alle Mitarbeitenden der KESB und all diejenigen, die in ihrem Auftrag tätig sind, und betrifft alle Informationen eines laufenden Verfahrens. Sie geht somit weiter als das Amtsgeheimnis.

Die Durchbrechung der Schweigepflicht ist im Gesetz nur in vier Fällen vorgesehen. Art. 451 Abs. 1 ZGB sieht eine Ausnahme von der Schweigepflicht vor, wenn ihr überwiegende Interessen der betroffenen Person, Dritter oder der Öffentlichkeit entgegenstehen. In Absatz 2 Art. 451 ZGB ist festgehalten, dass Dritten Auskunft über das Vorliegen und den Umfang einer Massnahme erteilt wird, wenn sie ein berechtigtes Interesse glaubhaft machen können. Gemäss Art. 453 ZGB sind alle involvierten Stellen sowie Polizei und KESB zur Zusammenarbeit verpflichtet, wenn eine akute Gefahr besteht, dass die betroffene Person sich oder Dritte schädigt. Schliesslich ist die Durchbrechung der Schweigepflicht möglich, wenn die betroffene Person einwilligt.

Umfassende Amtshilfe

Im Rahmen ihrer Abklärungen benötigt die KESB auch Informationen von anderen öffentlichen Organen. Diese sind zur Amtshilfe verpflichtet. Stehen keine schutzwürdigen Interessen entgegen, haben Verwaltungsstellen für die Aufgabenerfüllung der KESB alle notwendigen Akten herauszugeben,

Bericht zu erstatten und Auskunft zu erteilen. Ausgenommen sind Trägerinnen und Träger eines Berufsgeheimnisses. Ärztinnen und Zahnärzte, Apotheker, Hebammen und ihre Hilfspersonen nur zur Mitwirkung verpflichtet, wenn die vorgesetzte Stelle sie vom Berufsgeheimnis entbindet oder die betroffene Person einwilligt. Seit April 2013 fallen Psychologinnen und Psychologen ebenfalls unter das Berufsgeheimnis. Daraus ergeben sich bei der Auslegung der Bestimmungen über die Amtshilfe weitere Fragen. So ist nach dem derzeitigen Kindes- und Erwachsenenschutzrecht zum Beispiel nicht abschliessend geklärt, ob sich Schulpsychologinnen und -psychologen, die zusätzlich dem Amtsgeheimnis unterstehen, auch vom Berufsgeheimnis entbinden lassen müssen. De lege ferenda ist geplant, die Psychologinnen und Psychologen in Art. 448 ZGB explizit zu erwähnen.

Einzelfälle aus der Praxis

An einer Schule reichte eine Lehrperson eine Gefährdungsmeldung wegen häuslicher Gewalt bei der KESB ein. Die Schule wandte sich an den Datenschutzbeauftragten mit der Frage, ob die KESB den Eltern Einsicht in die Gefährdungsmeldung gewähren darf. Grundsätzlich haben alle Personen das Recht auf Zugang zu den sie betreffenden Personendaten, sofern der Auskunft keine überwiegenden privaten oder öffentlichen Interessen entgegenstehen. Als überwiegendes Interesse könnte dem Recht auf Zugang zu den eigenen Personendaten das Geheimhaltungsinteresse des Absenders entgegenstehen. Der Datenschutzbeauftragte hat deshalb festgehalten, dass die KESB eine Interessenabwägung vornehmen muss. Dabei ist auch denkbar, dass nur Teile der Gefährdungsmeldung oder anstelle des Originaldokuments ein Bericht über seinen Inhalt bekanntgegeben werden.

In einer weiteren Anfrage wandte sich das Volksschulamt an den Datenschutzbeauftragten mit der Frage, ob die KESB aufgrund einer Gefährdungsmeldung einer Schule betreffend einen Schüler von sich aus bei einer zweiten Schule Auskunft über den Bruder des Schülers einholen kann. Die KESB ermittelt den Sachverhalt von Amtes wegen. Es spielt also grundsätzlich keine Rolle, ob die KESB aufgrund einer Gefährdungsmeldung oder aufgrund eigener Ermittlungen tätig wird. Öffentliche Organe sind dabei zur Mitwirkung verpflichtet und müssen die für eine zu prüfende Massnahme rechtserheblichen Auskünfte erteilen. Sowohl bei der Auskunftserteilung wie auch bei einer allfälligen zwangsweisen Durchsetzung ist das Verhältnismässigkeitsprinzip zu beachten. Weiter kann der Mitwirkung ein Berufsgeheimnis der angefragten Stelle entgegenstehen. Der Datenschutzbeauftragte hielt deshalb fest, dass die betroffene Schule prüfen muss, ob die Auskunft erteilende Person dem Berufsgeheimnis untersteht, dass sie grundsätzlich aber zur Mitwirkung verpflichtet sei.

Art. 446 ZGB
Art. 448 ZGB
Art. 451 Abs. 1 ZGB
Art. 451 Abs. 2 ZGB
Art. 453 ZGB

Datenschutz in der Schule – die tägliche Herausforderung

Wenn es um das Thema «Datenschutz und Privatsphäre» geht, sind Lehrerinnen und Lehrer im Schulalltag genauso gefordert wie Schülerinnen und Schüler. Der Nutzung der neuesten Technologien im Schulalltag steht nichts entgegen, wenn die entsprechenden Voraussetzungen beachtet werden.

Der Datenschutzbeauftragte hat mit zahlreichen Schulen auf Mittelschulebene zusammengearbeitet. In direktem Dialog mit Schülerinnen und Schülern wurde das Thema Datenschutz erörtert – sei dies, was die Nutzung sozialer Medien betrifft oder ganz allgemein die Privatsphäre. Im Zentrum der Aktivitäten stand das Bestreben, das Bewusstsein für den Wert der Privatsphäre und der Kontrolle der eigenen Daten zu fördern und zu verankern. Nur wenn Lernende die Frage beantworten können, warum sie ihre Daten schützen sollen, kann in Bezug auf den Datenschutz etwas erreicht werden. Medienkompetenz und Datenschutz sollten deshalb in den Schulen möglichst früh und systematisch vermittelt werden.

Einsatz von Spezialprogrammen und sozialen Medien

In der Beratungstätigkeit haben Lehrpersonen schwerpunktmässig Fragen zur Nutzung verschiedener Programme und zur Auslagerung von Daten an Dritte gestellt. Diese Anwendungen, beispielsweise LehrerOffice, ermöglichen zwar eine effiziente Bewältigung der Datenmenge im Schulbereich, dabei geht aber ob der Attraktivität oft vergessen, dass nicht unbedingt erlaubt ist, was nicht explizit verboten ist. So ist es ein Muss, vor jeder Auswahl eines solchen Produkts zu analysieren, welche Daten zu welchem Zweck gestützt auf welche Rechtsgrundlagen bearbeitet werden dürfen. Enthält eine Anwendung Datenkategorien, die sich mit der Aufgabenerfüllung respektive der Rechtsgrundlage nicht vereinbaren lassen, dürfen diese Informationen nicht bearbeitet werden. Beispielsweise dürfen mit LehrerOffice nur die in der Bildungsdatenverordnung aufgeführten Datenkategorien elektronisch erfasst und bearbeitet werden. Die meisten dieser Produkte werden von Firmen angeboten, welche die Daten im Auftragsverhältnis bearbeiten. Deshalb müssen die Verträge und die Allgemeinen Geschäftsbedingungen der Anbieter mit den Anforderungen des Datenschutzes abgeglichen werden. In vielen Fällen steht der Nutzung die Auslagerung der Daten in eine Cloud im Weg, weil keine Gewähr besteht, dass sie zweckgebunden verwendet werden oder beispielsweise bei besonderen Personendaten keine Verschlüsselung möglich ist. Weitere Informationen dazu finden sich im Merkblatt «Cloud Computing im Schulbereich» von privatim, der Vereinigung der kantonalen Datenschutzbeauftragten, sowie im Merkblatt «Online-Speicherdienste» des Datenschutzbeauftragten (www.datenschutz.ch.)

Die Fragen ob soziale Medien wie Facebook etc. von Lehrpersonen im Unterricht benutzt werden dürfen und worauf zu achten ist, beantwortet ein weiteres Merkblatt von privatim: Es ist insbesondere darauf zu achten, dass im Bereich der interaktiven Kommunikation keine besonderen Personendaten von anderen Lernenden ausgetauscht werden. Es braucht also eine vorgängige Instruktion, wie mit sensiblen Daten umgegangen werden soll.

Publikationen im Internet

Ein Dauerbrenner bei den Anfragen ist, welche Informationen im Internet publiziert werden dürfen. Recherchen des Datenschutzbeauftragten, welche gestützt auf eine Anfrage eines Vaters erfolgten, haben eine äusserst heterogene Handhabung durch die Schulen zu Tage gefördert. Teilweise werden sogar Portraits von Kindern mit vielen Details wie Hobbys, Lieblingsessen usw. publiziert, auch Fotos von Schwimmbadbesuchen im Klassenverband waren keine Seltenheit. Die Sensibilisierung in diesem Bereich ist nicht abgeschlossen.

Weiterleitung von Informationen

Immer wieder werden Fragen zur Weiterleitung von Informationen gestellt, beispielsweise bei einem Übertritt in eine neue Klasse. Oft ist das Berufsgeheimnis betroffen, dem die Schulpsychologinnen und -psychologen unterstellt sind. In solchen Fällen ist meist das Einverständnis der Eltern einzuholen. Falls es verweigert wird, können eventuell im Rahmen der Amtshilfe die für die Aufgabenerfüllung erforderlichen Informationen bekannt gegeben werden. Jeder Sachverhalt ist detailliert und einzeln zu prüfen.

Die beiden Seiten der Medaille

Das Informations- und Datenschutzgesetz (IDG) hat zwei Schwerpunkte: den Datenschutz und das Öffentlichkeitsprinzip. Sie sind im Bewusstsein der Bevölkerung unterschiedlich präsent.

Im Rahmen der etappenweisen Evaluation des IDG (siehe auch Tätigkeitsbericht 2012, Seite 12) lag der erste Themenschwerpunkt bei der Sensibilisierung der Bevölkerung. Datenschutz und Informationszugang sind die beiden Seiten derselben Medaille, weshalb das IDG beide Materien aufeinander abgestimmt regelt. Fünf Jahre nach Inkraftsetzung des IDG stellen sich in diesem Evaluationsschritt Fragen, wie sich die Bevölkerung zum Datenschutz im allgemeinen sowie zum Öffentlichkeitsprinzip und zum Recht auf Informationszugang stellt. Weiter sollten das Vertrauen in die öffentlichen Organe erfasst und die Kenntnisse in Bezug auf die Datenschutzrechte und das Recht auf Informationszugang erfragt werden. Weiter war von Interesse, wie weit die Bevölkerung die fachspezifischen Organe im Bereich des Datenschutzes und des Informationszugangs kennt.

Repräsentative Umfrage

In Zusammenarbeit mit dem statistischen Amt wurde eine repräsentative Umfrage konzipiert und von einem spezialisierten Institut bei der Bevölkerung im Kanton Zürich durchgeführt. Ziel war es, alle Bevölkerungsschichten und Alterskategorien anzusprechen. Die Resultate wurden vom statistischen Amt ausgewertet und werden in die Gesamtevaluation des IDG einfliessen. Ein summarischer Überblick zeigt folgende Resultate:

Bereich Datenschutz

- In allen Alterskategorien wird der Schutz der persönlichen Daten als sehr wichtig eingestuft (Mittelwert 8,4 auf einer Skala von 1 bis 10). Über 80 Prozent der Bevölkerung beurteilen den Stellenwert des Datenschutzes in der öffentlichen Diskussion als gerechtfertigt und fast die Hälfte ist der Meinung, dass er noch mehr thematisiert werden müsste.
- Die Mehrheit der Bevölkerung vertraut der öffentlichen Verwaltung, dass Personendaten korrekt bearbeitet werden. Das Vertrauen variiert aber zwischen den Institutionen.
- Über 80 Prozent der Bevölkerung wissen, dass sie jederzeit das Recht auf Auskunft über ihre eigenen Daten bei einem öffentlichen Organ wahrnehmen können.
- Rund 60 Prozent der Bevölkerung wissen, dass im Kanton Zürich eine Behörde für den Daten-

schutz zuständig ist, und rund 40 Prozent kennen die korrekte Bezeichnung «Datenschutzbeauftragter».

Bereich Öffentlichkeitsprinzip

- In allen Alterskategorien wird das Öffentlichkeitsprinzip als wichtig eingestuft (Mittelwert 7,7 auf einer Skala von 1 bis 10).
- 40 Prozent der Bevölkerung wissen, dass es ein Recht auf Informationszugang gibt, aber weniger als die Hälfte weiss, dass es ohne Begründung geltend gemacht werden kann.
- Rund ein Drittel der Bevölkerung glaubt, dass es im Kanton Zürich eine Behörde für das Öffentlichkeitsprinzip gibt. 80 Prozent können keinen Namen nennen oder bezeichnen andere (u.a. Datenschutzbeauftragter, Ombudsmann, Staatskanzlei) als zuständig.

Schrittweise Evaluation geht in den kommenden Jahren weiter

Die Evaluation des IDG wird in den Jahren 2014 bis 2017 weiter geführt, und dies mit jeweils unterschiedlichen Themenschwerpunkten. 2014 wird untersucht, ob in den sensiblen Bereichen wie Polizei oder Gesundheitswesen hinreichend bestimmte formell-gesetzliche Grundlagen für alle Datenbearbeitungen bestehen. Ein Jahr später steht die Wirksamkeit der Aufsicht im Hinblick auf den Informationszugang und den Datenschutz auf dem Programm des Evaluationsteams und 2016 soll untersucht werden, wie die öffentlichen Organe im Kanton Zürich über das Öffentlichkeitsprinzip und den Datenschutz informieren. Abschliessend sollen 2017 in einer Evaluationssynthese die Erkenntnisse aus den verschiedenen geprüften Bereiche zu einer Gesamtschau über die vielfältigen Wirkungen des IDG zusammen geführt werden.

Datenschutzbeauftragter

Nr. 9071
Funktionale Gliederung: 0

Finanzierung

Erfolgsrechnung (in Mio. Fr.)	R 12	B 13	Δ(P 14)	P 14	Δ(P 15)	P 15	Δ(P 16)	P 16	P 17	Δ%(12-17)
Ertrag	0.0	0.1	-0.0	0.1	-0.0	0.1	-0.0	0.1	0.1	
Aufwand	-2.1	-2.3	-0.0	-2.4	-0.0	-2.3	-0.0	-2.4	-2.4	14.9
Saldo	-2.1	-2.2	-0.1	-2.3	-0.1	-2.3	-0.1	-2.3	-2.3	
Investitionen (in Mio. Fr.)										Ø (12 -17)
Einnahmen										
Ausgaben		-0.1								-0.0
Nettoinvestitionen		-0.1								-0.0
Personal (Beschäftigungsumfang)	8.8	9.2	0.0	9.2	0.0	9.2	0.0	9.2	9.2	

Aufgaben

A1 Der Datenschutzbeauftragte beaufsichtigt die Datenbearbeitungen der kantonalen Verwaltung, der Gemeinden und der übrigen Behörden und öffentlichen Einrichtungen im Kanton, um die Privatheit der Bürgerinnen und Bürger sicher zu stellen.

A2 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.

A3 Bei öffentlichen Organen überprüft er mittels Kontrollen (Datenschutz-Reviews), ob die Anforderungen des Datenschutzes in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht eingehalten sind.

A4 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.

Entwicklungsschwerpunkte

		bis
E1	Gesetzeskonformer Umgang mit Personendaten in sensitiven Bereichen fördern und fordern (Gesundheitswesen, Schule, Sozialbereich etc.)	2014
E2	Förderung der Umsetzung angemessener Massnahmen im Bereich der Informationssicherheit	2015
E3	Sicherstellen des Datenschutzes im Umgang mit grossen Datenmengen (eGovernment, Open Government Data, Forschung, Big Data)	2016

Indikatoren

Indikatoren	Art	R 12	B 13	P 14	P 15	P 16	P 17
Wirkungen							
W1 Anteil umgesetzter Hinweise bei Datenschutz-Reviews (%) (A3)	min.	34	60	60	60	60	60
W2 Anzahl Besuche auf Webseiten (A4)	min.	112670	80'000	80'000	80'000	80'000	80'000
Leistungen							
L1 Anzahl Beratungen von Privatpersonen (A4)	max.	434	500	500	500	500	500
L2 Anzahl Vernehmlassungen und Mitberichte (A2)	P	11	18	18	18	18	18
L3 Anzahl Weiterbildungsangebote für öffentliche Organe (A2)	min.	19	15	15	15	15	15
L4 Anzahl Kontrollen (A3)	min.	18	30	30	30	30	30
Wirtschaftlichkeit							

Leistungsgruppe 9071	Budgetentwurf 2014
Budgetkredit Erfolgsrechnung (in Mio Fr.)	-2.299
Budgetkredit Investitionsrechnung (in Mio. Fr.)	
Leistungsindikatoren L1, L3 und L4	

Budget	Leistungsgruppe 9071
Vom Budgetentwurf abweichende Budgetbeschlüsse des KR können hier eingeklebt werden	

Mobil, aber sicher

Die mobile Datenbearbeitung der Zukunft bringt viele neue Möglichkeiten, aber auch neue Risiken. Medienkompetenz ist gefragt.

Bereits heute werden von einzelnen öffentlichen Organen mobile Geräte wie Smartphones oder Tablets flächendeckend eingesetzt. Sie ermöglichen orts- und zeitunabhängig den Zugriff auf Daten und deren Bearbeitung. Ihr Einsatz erfordert zusätzliche Sicherheitsmassnahmen, um den Schutz der Daten gleichermassen zu gewährleisten wie am Arbeitsplatz.

Auch in der Bevölkerung nimmt die Nutzung von mobilen Geräten laufend zu und viele Interaktionen mit der Verwaltung erfolgen bereits mit solchen Geräten. Auch hier sind Massnahmen zum Schutz der persönlichen Daten notwendig.

In beiden Fällen ist aber auch zu beachten, dass die Nutzung mobiler Geräte zur Erfassung weiterer Daten führt. Beim Aufbau der Kommunikation und bei der Verwendung einzelner Applikationen werden Metadaten erfasst, die Auskunft geben über Ort, Zeit oder Inhalt der Kommunikation. Dabei bleibt intransparent, wer (Hersteller des Geräts, Telekommunikationsanbieter, Applikationsanbieter etc.) was (Aufbewahren, Löschen, Auswerten etc.) mit den Daten macht. In der sich abzeichnenden Zukunft des «Internets der Dinge» werden vermehrt auch andere «Objekte (Geräte, Gegenstände etc.) mit dem mobilen Gerät Kontakt aufnehmen, um Daten auszutauschen – wie, in welcher Form und zu welchem Zweck bleibt auch hier offen.

Diese Situation verlangt von den öffentlichen Organen vermehrte Kompetenz im Bereich der Sicherheit: Auch im smarten Umfeld des Internets der Dinge sind die Daten der Bürgerinnen und Bürger zu schützen.

Aber auch die Bürgerinnen und Bürger werden vermehrt gefragt sein. Sie müssen lernen, kompetent mit diesen Geräten umzugehen, sich aber auch bewusst werden, warum und wie sie ihre persönlichen Daten schützen wollen.

Die neuen Technologien in der mobilen Welt bringen Chancen, die aber nicht die Risiken verdecken dürfen. Die Risiken sind direkt zu adressieren und so weit wie möglich zu minimieren. Die allgegenwärtige Datenbearbeitung ist eine Herausforderung für den Schutz und die Sicherheit der Daten, aber auch für die informationelle Selbstbestimmung und den Schutz der Privatsphäre. Ein wirkungsvoller Datenschutz bleibt angesichts dieser technologischen Entwicklung auch in Zukunft dringend nötig.

1 Jubiläum, 2 Checklisten, 3 Merkblätter und 4 Hashtags

Die Volksabstimmung über das Datenschutzgesetz vor zwanzig Jahren, Hilfestellungen für mehr Informationssicherheit im Arbeitsalltag und eine kontinuierliche Weiterentwicklung der Kommunikation via Twitter – diese Themen bildeten Schwerpunkte der Informationstätigkeit des Datenschutzbeauftragten.

Anlässlich des 20. Jahrestages der Volksabstimmung über das Datenschutzgesetz vom Juni 1993 führte der Datenschutzbeauftragte am 4. Juni eine Veranstaltung unter dem Titel «Vom Wert der Privatheit» durch, um über die aktuellen und zukünftigen Herausforderungen des Schutzes der Privatsphäre zu debattieren. Rund hundert Vertreterinnen und Vertreter aus Politik, Verwaltung, Wirtschaft sowie Forschung und Lehre nahmen an der halbtägigen Jubiläumsveranstaltung teil. Höhepunkt bildete ein Referat über die Entwicklung hin zu umfassenden Datenbearbeitungen, in der Mensch, Internet und Realität zunehmend verschmelzen und bei der das Smartphone als Mediator zwischen den Hauptprotagonisten fungiert. Faltbare Computer, hochauflösende Displays oder Apps zur informationellen Anreicherung der via Smartphone abgebildeten Realität sind nur einige Elemente, die die Fähigkeiten und Wahrnehmungen der Menschen in einer Art und Weise erweitern, die die Technik unwiderstehlich erscheinen lässt. Diese Unwiderstehlichkeit bringt für den Datenschutz ganz neue und ungeahnte Herausforderungen mit sich. Die Diskutanten des abschliessenden Podiums waren sich deshalb einig, dass vor diesem Hintergrund das Konzept von Privatheit einer breiten öffentlichen Debatte bedarf. Dem Datenschutzbeauftragten kommt dabei eine zentrale Rolle bezüglich Aufklärung der öffentlichen Organe und der Bevölkerung über die Chancen und Risiken der neuen technologischen Möglichkeiten zu.

Neue Checklisten für mehr Informationssicherheit

Die zahlreichen Geschäfte und Anfragen im Bereich Informationssicherheit veranlassten den Datenschutzbeauftragten, zwei neue Checklisten zu veröffentlichen: Die Checkliste «Löschung Suchmaschinen-Cache» zeigt auf, wie sich die bei Internetrecherchen noch längere Zeit in öffentlich zugänglichen Web-Zwischenspeichern (Caches) gespeicherten Informationen der drei grossen Suchmaschinen Google, Bing und Yahoo löschen lassen. Die Checkliste «Webtracking verhindern» legt dar, mit welchen organisatorischen Massnahmen und Browsereinstellungen der Aufzeichnung und Auswertung des Besucherverhaltens auf Websites entgegengewirkt werden kann.

Praktische Hilfestellungen für den Arbeitsalltag

Die neuen datenschutzrechtlichen Herausforderungen bei der verstärkten Nutzung von Webdiensten aller Art bewegten den Datenschutzbeauftrag-

ten, auch das Angebot an Merkblättern zu erweitern. Das Merkblatt «Online-Speicherdienste» enthält eine Übersicht über die wichtigsten datenschutzrechtlichen Anforderungen sowie eine Risikoanalyse der bekanntesten Anbieter von Online-Speicherdiensten; das Merkblatt «Online-Recherchen über Stellenbewerber» informiert darüber, in welchen Fällen ein öffentliches Organ als Arbeitgeberin im Bewerbungsverfahren Informationen über Stellenbewerbende aus dem Internet und aus sozialen Netzwerken erheben und verwenden darf. Ergänzt werden die beiden Publikationen durch das Merkblatt «Informationsverwaltung», das den Mitarbeitenden von öffentlichen Organen klar und einfach aufzeigt, wie Grundsätze der Informationsverwaltung in der Aktenführung eingehalten werden können.

Alle Publikationen können auf www.datenschutz.ch unter der Rubrik «Veröffentlichungen» heruntergeladen werden.

#Datenschutz, #Privacy, #Informationssicherheit, #Security

Die vier Hashtags #Datenschutz, #Privacy, #Informationssicherheit und #Security dominierten auch 2013 die vom Datenschutzbeauftragten auf Twitter publizierten Informationen. Über Twitter wurden eigene News publiziert, aber auch auf Inhalte von Experten und Partnerinstitutionen hingewiesen. Insgesamt entwickelte sich die Kommunikation über den Ende 2012 lancierten Social-Media-Kanal erfreulich: Eine steigende Anzahl Follower sowie vermehrte Retweets und Rückmeldungen oder via Twitter eingegangene Anfragen haben den Austausch mit den Zielgruppen intensiviert. Der Datenschutzbeauftragte hat sich deshalb entschlossen, diesen Kanal auch in Zukunft zu verwenden und ihn schrittweise auszubauen. Auf einen Facebook-Auftritt soll hingegen vorläufig verzichtet werden.

Dem Twitter-Account des Datenschutzbeauftragten kann unter @dsb_zh gefolgt werden.

Symposium ganz im Zeichen der Datenberge

Big Data stand im Zentrum des 18. Symposiums on Privacy and Security, das die Stiftung für Datenschutz und Informationssicherheit wiederum Ende August durchführte. Die unglaublichen Datenmengen, die in Verwaltung und Wirtschaft, aber auch im Internet unaufhaltsam wachsen, werden immer gründlicher ausgewertet – auch personenbezogen. Es herrscht eine wahre Goldgräberstimmung beim so genannten «Data Mining» in den wachsenden Datenbergen. Das Symposium stellte sich dem Thema und diskutierte die Frage, ob das heutige Datenschutzrecht diesen Herausforderungen noch genügt oder welcher gesetzgeberischer und/oder gesellschaftlicher Handlungsbedarf besteht.

Erfolgreiche Seminare, Kurse und Referate

Die Nachfrage nach Weiterbildungen und themenspezifischen Präsentationen war 2013 unverändert gross. Insbesondere im Bildungsbereich hielt der Datenschutzbeauftragte eine Vielzahl von Referaten.

Der Datenschutz wird vermehrt zum Thema im Unterricht von Kantons- und Berufsschulen. Der Datenschutzbeauftragte wurde von mehreren Schulen angefragt, im Rahmen von Projektwochen oder -tagen ein Referat zu halten. Angesichts der rasanten Zunahme von Social Media und Smartphone-Applikationen ist die Sensibilisierung von Jugendlichen für den Datenschutz und den Schutz ihrer Privatsphäre enorm wichtig und ein Schwerpunkt der Tätigkeit des Datenschutzbeauftragten (siehe auch Seiten 12/13).

Seminarangebot

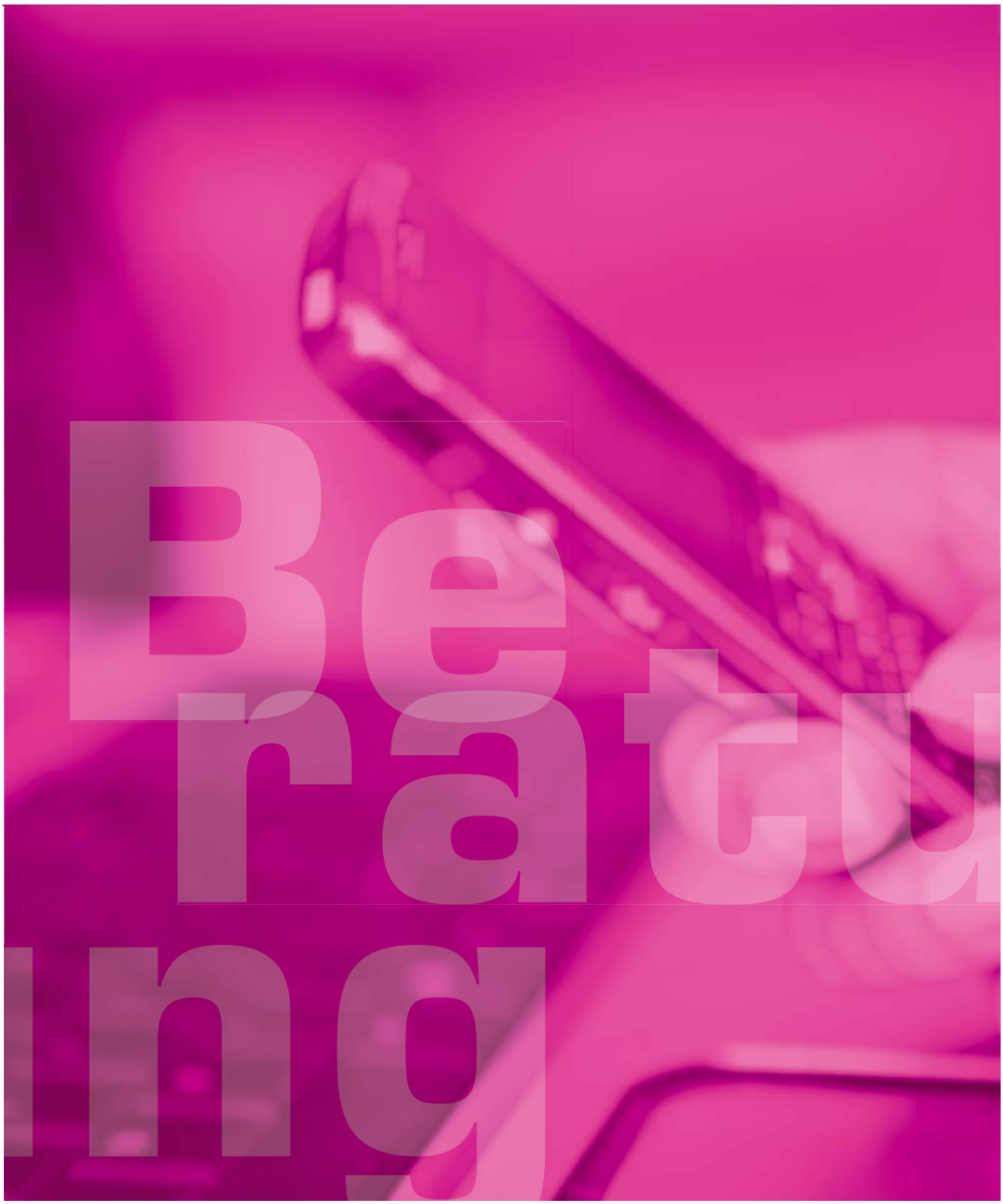
Seit vielen Jahren bietet der Datenschutzbeauftragte Seminare für verschiedene Zielgruppen an. Die Seminare bauen auf einem bewährten Lernprogramm auf, das im Internet frei zugänglich ist und anhand vieler Beispiele, Fälle und eines Quiz einen ersten, praxisnahen Einstieg in die Materie ermöglicht. Im Rahmen von Vertiefungsseminaren für Juristinnen und Juristen, Mitarbeitende im Sozialbereich und im Gesundheitswesen werden fachspezifische Fragen behandelt. Ein grosser Anteil der Unterrichtszeit steht für Übungen anhand von Fallkonstellationen zur Verfügung, so dass ein enger Bezug zum Alltag der Teilnehmenden gewährleistet ist. Auch das Seminar zum Öffentlichkeitsprinzip konnte zusammen mit der Koordinationsstelle IDG der Staatskanzlei wieder erfolgreich durchgeführt werden.

Sicherheitskurse

Datenschutz und Informationssicherheit gehen Hand in Hand. 2013 wurden deshalb wiederum Kurse für Informatikverantwortliche angeboten. Diese waren spezifisch auf die Bedürfnisse von Spitex-Organisationen, Alters- und Pflegeheimen zugeschnitten. Diesen oft eher kleinen Organisationen stehen für den Informatikbetrieb nur wenig Ressourcen zur Verfügung. Gleichwohl finden sensible Datenbearbeitungen statt. An den Kursen erhielten die für die Informatik verantwortlichen Mitarbeitenden spezifische Hilfestellungen zur Verbesserung des Sicherheitsniveaus in ihrem jeweiligen Bereich.

Module in Zertifikatskursen

Der Datenschutz ist vermehrt auch ein Thema in Zertifikats- und Diplomkursen von Hochschulen. Bereits seit einiger Zeit referiert der Datenschutzbeauftragte in einem Modul zum Datenschutz im Bereich der klinischen Forschung (Zertifikatskurs CAS Clinical Trial Management des Universitätsspitals Zürich). Ein ganztägiges Modul zum Datenschutz im Sozialwesen fand 2013 erstmals im Zertifikatskurs (CAS) Kindes- und Erwachsenenschutzrecht der ZHAW Zürcher Hochschule für angewandte Wissenschaften statt.



«Die Publikation von Fotos im Internet sollte vom ethischen Grundsatz geleitet werden, dass nicht alles, was veröffentlicht werden kann, auch tatsächlich veröffentlich werden soll.»

Durchsetzung eigener Rechte und Anwendung neuer Gesetze

Die Anfragen der Bürgerinnen und Bürger betrafen hauptsächlich die Durchsetzung der eigenen Rechte wie das Recht auf Auskunft, Berichtigung und Löschung. Schwerpunkt bei den öffentlichen Organen waren die Themen Auslagerung, insbesondere im Zusammenhang mit Cloud Computing, der Einsatz von Videokameras, die Umsetzung des neuen Kindes- und Erwachsenenschutzrechts sowie die Publikation von Fotos im Internet.

Mehrere Personen wandten sich an den Datenschutzbeauftragten, weil sie im Rahmen der Geltendmachung ihrer Rechte von der angefragten Behörde keine Auskunft erhielten. So hat der Datenschutzbeauftragte Fälle bearbeitet, bei denen Gemeinden bei einer Einschränkung oder Verweigerung einer Auskunft keine vom IDG vorgesehene Verfügung erlassen hatten. Bei Ersuchen auf Löschung von Patientendaten muss vom öffentlichen Organ zudem berücksichtigt werden, dass gemäss Gesundheitsgesetz eine zehnjährige Aufbewahrungspflicht besteht. Allenfalls unrichtige Patientendaten können durch Ergänzungen berichtigt werden.

Fragen zur Umsetzung des neuen Kindes- und Erwachsenenschutzrechts wurden von Privatpersonen wie auch von Behörden gestellt. Im Fokus der Beratung und damit der Auslegung des Gesetzes stand die der Kinder- und Erwachsenenschutzbehörde auferlegte Schweigepflicht. Diese kann nur im Rahmen der vom ZGB festgelegten Sachverhalte oder bei Vorliegen einer Einwilligung der betroffenen Person durchbrochen werden. Eine allgemeine Amtshilfebestimmung genügt nicht.

Weitere Anfragen der Verwaltung betrafen die Videoüberwachung und die Publikation von Fotos, insbesondere von Schülerinnen und Schülern, im Internet. Zum Ersteren wurden mehrere Anfragen zum Verkehrsmonitoring mittels Einsatz von Videokameras gestellt; grundsätzlich gelten hierfür dieselben Voraussetzungen wie für eine Videoüberwachung. Publikationen von Schülerfotos im Internet bedürfen der Einwilligung der Eltern oder der urteilsfähigen Kinder. Zu berücksichtigen sind neben der Verhältnismässigkeit auch ethische Aspekte. So sollte zum Wohl der Kinder und Jugendlichen nicht alles publiziert werden, was veröffentlicht werden kann (Schwimmbadfotos, Portraits, Informationen über Hobbys usw.)

Weitere Themen waren die Auslagerung von Datenbearbeitungen unter Inanspruchnahme einer Cloud, beispielsweise beim Einsatz von Kinderdiagnosetools. In diesem Zusammenhang sind auch die Verhandlungen von privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, mit Microsoft zu erwähnen, bei denen erreicht werden konnte, dass Microsoft eine Vertragsergänzung akzeptiert hat, die eine datenschutzkonforme Nutzung von Office 365 im Schulbereich gewährleistet.

Einige wichtige Fälle werden auf den folgenden Seiten ausführlich vorgestellt.

01
Einsicht von Privatversicherungen in Akten von Strafverfahren

Die Oberstaatsanwaltschaft gelangte mit der Frage an die Koordinationsstelle IDG der Staatskanzlei, unter welchen Voraussetzungen Privatversicherungen Einsicht in Akten abgeschlossener Strafverfahren erhalten. So benötigen zum Beispiel Haftpflichtversicherungen zur Schadensregulierung bei Verkehrsunfällen oft Informationen aus den Strafakten, beispielsweise Einsicht in die Polizeirapporte. Da diese Frage Aspekte sowohl des Öffentlichkeitsprinzips als auch des Datenschutzes betraf, wandte sich die Koordinationsstelle IDG an den Datenschutzbeauftragten.
Nach Abschluss eines Strafverfahrens richtet sich das Akteneinsichtsrecht nach dem IDG. Das IDG sieht für die Frage des Akteneinsichtsrechts von Privatversicherungen jedoch keine befriedigende Lösung vor. Das Recht auf Zugang zu den eigenen Personendaten ist nicht zielführend, da die Informationen, welche der Privatversicherer benötigt, in der Regel nicht erfasst sind. Das Recht auf Zugang zu Informationen nach dem Öffentlichkeitsprinzip erfordert die Anhörung sämtlicher von der Akteneinsicht betroffener Personen. Häufig können aber gar nicht alle Betroffenen kontaktiert werden. Ausserdem kann das Verfahren zu stossenden Ergebnissen führen, da es der Beschuldigte oder andere Betroffenen in der Hand haben, die Einsicht zu verhindern, obwohl die Privatversicherung ein berechtigte Einsichtsinteresse hat.
Die Frage ist deshalb anders zu lösen. Das Bundesgericht anerkennt in konstanter Praxis das Recht auf Akteneinsicht als Teilgehalt des Anspruchs auf rechtliches Gehör. Betroffene und Dritte haben Anspruch auf Einsicht in die Akten eines abgeschlossenen Verfahrens, sofern sie ein besonderes schutzwürdiges Interesse glaubhaft machen können. Das Akteneinsichtsrecht findet seine Grenzen an überwiegenden öffentlichen Interessen des Staates oder an berechtigten Interessen Dritter. Dieser verfassungsrechtliche Anspruch ist eine Minimalgarantie, welche direkt anwendbar ist und dem IDG vorgeht bzw. dieses ergänzt. Der Datenschutzbeauftragte gelangte deshalb zum Schluss, dass den Privatversicherungen die Einsicht in Strafakten gestützt auf Art. 29 BV gewährt werden kann.

Art. 99 StPO
Art. 29 BV
§ 20 Abs. 1 und 2 IDG
§ 26 IDG

02
Auskunftsrecht umfasst auch Logdaten

Eine Privatperson gelangte an den Datenschutzbeauftragten, weil ihr die Kantonspolizei die Einsicht in die Logdaten bezüglich eines Eintrags im Polizeiinformationssystem POLIS verweigerte. Die betroffene Person vermutete, dass an einem Dokument unzulässigerweise Änderungen vorgenommen worden waren. Daher wollte sie wissen, wer wann auf die Daten zugegriffen bzw. wer diese Daten in welcher Weise bearbeitet hatte.
Die Kantonspolizei verweigerte der betroffenen Person zunächst die Einsicht in die Logdaten mit der Begründung, dass die POLIS-Logdaten verwaltungsinterne Fallführungsdaten seien, die den organisatorisch-administrativen Bereich des polizeilichen Handelns beträfen. Die Kantonspolizei qualifizierte das Gesuch der betroffenen Person als Gesuch um verfahrensrechtliche Akteneinsicht und nicht als Auskunftsgesuch im

Sinn der Datenschutzgesetzgebung. Das Akteneinsichtsrecht bezieht sich lediglich auf Akten, welchen in einem Verfahren Beweischarakter zukommt und die dazu dienen, einen Entscheid zu begründen. Im Unterschied dazu erstreckt sich das Auskunftsrecht auf sämtliche Daten, welche ein öffentliches Organ über eine Person aufgezeichnet hat, also auch auf interne Akten.
Der Datenschutzbeauftragte wies die Kantonspolizei deshalb darauf hin, dass Logdaten im Zusammenhang mit Zugriffen auf die in POLIS gespeicherten Informationen personenbezogene Daten sind und somit vom Recht auf Einsicht in die eigenen Daten umfasst werden. Die Namen der zugreifenden Personen sind grundsätzlich offenzulegen, wenn im Einzelfall keine überwiegenden Geheimhaltungsinteressen bestehen. Ob die Kantonspolizei die betroffenen Mitarbeitenden vor dem Entscheid anhören will, ist ihr überlassen. Verweigert die Kantonspolizei die Einsicht, schränkt sie diese ein oder schiebt sie diese auf, hat sie eine Verfügung zu erlassen.
Die Kantonspolizei teilte diese Rechtsauffassung und erliess eine Verfügung. Damit erhielt die betroffene Person die Möglichkeit, die Einschränkung des Auskunftsrechts gerichtlich überprüfen zu lassen.

§ 20 Abs. 2 IDG
§ 23 IDG
§ 26 IDG
§ 27 IDG

03
Schülerportraits im Internet

Eine Schule veröffentlichte zahlreiche Fotos von Kindern, teilweise mit Namen und anderen Informationen zu den persönlichen Lebensumständen wie Hobbys und Berufswunsch, auf ihrer Website. Die Fotos waren über einen längeren Zeitraum recherchierbar. Ein betroffener Elternteil wandte sich an den Datenschutzbeauftragten mit dem Anliegen, die Zulässigkeit dieser Praxis im Hinblick auf die datenschutzrechtlichen Anforderungen zu überprüfen.
Die Veröffentlichung von Fotos von Schülerinnen und Schülern im Internet stellt eine Bekanntgabe von Personendaten dar. Diese bedarf einer gesetzlichen Grundlage oder der Einwilligung der Betroffenen. Für die Publikation von Personendaten von Schülerinnen und Schüler besteht keine gesetzliche Grundlage. Aus diesem Grund ist immer eine vorgängige Zustimmung der betroffenen Schülerin, des betroffenen Schülers bzw. deren Erziehungsberechtigten einzuholen. Selbst wenn eine Einwilligung vorliegt, sind die dem Internet inhärenten Risiken für die Verletzung der Persönlichkeitsrechte in die Entscheidung einzubeziehen, ob ein Foto veröffentlicht werden soll oder nicht. So können beispielsweise einmal im Internet publizierte Fotos nicht mehr komplett gelöscht und können unkontrolliert zu anderen Zwecken bearbeitet werden. Daraus folgt, dass bei Veröffentlichungen im Internet grösstmögliche Zurückhaltung geboten ist. Insbesondere Portraitaufnahmen und persönliche Daten von Kindern sowie Bilder von möglicherweise kompromittierenden Situationen (Ausflug ins Schwimmbad) sollten nicht im Internet veröffentlicht werden. Weiter ist durch die Schule sicherzustellen, dass die Fotos periodisch gesichtet und gelöscht werden.
Im beurteilten Fall entfernte die Schule die Portraits sowie weitere Fotos mit persönlichen Informationen. Die Schule erstellte sodann ein Datenschutzreglement für den Umgang mit den Personendaten ihrer Schülerinnen und Schüler.

§ 8 Abs. 1 IDG
§§ 16 / 17 IDG
§ 23 IDG

04
Neue Regeln zur Herausgabe der Patientendokumentation

Spitäler werden verschiedentlich mit Gesuchen um Herausgabe der Patientendokumentation im Original sowie Löschung der elektronischen Daten konfrontiert. Dabei stellt sich die Frage, ob das Spital die Patientendokumentation im Original herausgeben muss und ob die gängige Praxis, die Patientin bzw. den Patienten einen Haftungsverzicht unterzeichnen zu lassen, standhält. Als ein Spital mit dieser Frage an den Datenschutzbeauftragten gelangte, nahm dieser die Anfrage zum Anlass, die Frage der Herausgabe der Patientendokumentation in grundsätzlicher Hinsicht zu klären.
Das Patientinnen- und Patientengesetz des Kantons Zürich (PatG) regelt die Aufbewahrung und Herausgabe der Patientendokumentation von Behandlungen in Spitälern. Demnach ist die Patientendokumentation Eigentum des Spitals und darf nach Abschluss der letzten Behandlung während zehn Jahren aufbewahrt werden. Im Interesse der Patienten oder zu Forschungszwecken kann das Spital die Aufbewahrungsfrist auf dreissig Jahre oder, in Absprache mit dem zuständigen Archiv, auf fünfzig Jahre verlängern. Patientinnen und Patienten haben Anspruch auf Einsicht, soweit nicht schutzwürdige Interessen Dritter entgegenstehen. In diesem Umfang haben sie auch Anspruch auf die Abgabe von Kopien. Nach Ablauf der Aufbewahrungsfrist können sie die Herausgabe oder Vernichtung der Patientendokumentation verlangen, wenn diese vom zuständigen Archiv nicht übernommen wird oder keine Anbietepflicht an ein Archiv besteht. Der Anbietepflicht unterliegen Spitäler, welche öffentliche Aufgaben erfüllen. Die Herausgabe der Patientendokumentation an die Patientin bzw. den Patienten kann mit Rücksicht auf schutzwürdige Interessen Dritter eingeschränkt werden.
Der Datenschutzbeauftragte gelangte zum Schluss, dass Patientinnen und Patienten während der Aufbewahrungsfrist lediglich Kopien ihrer Patientendokumentation verlangen können, da die Herausgabe der Patientendokumentation im Original die Möglichkeit der Übernahme durch das zuständige Archiv vereiteln würde. Zudem dürfte die gängige Praxis, bei Herausgabe der Original-Patientendokumentation die Patientin bzw. den Patienten einen Haftungsverzicht unterzeichnen zu lassen, nicht standhalten. Nach Ablauf der Aufbewahrungsfrist darf das Spital der Patientin bzw. dem Patienten die Patientendokumentation hingegen herausgeben, sofern diese vom zuständigen Archiv nicht übernommen wird bzw. keine Anbietepflicht an ein Archiv besteht und soweit keine schutzwürdigen Interessen Dritter entgegenstehen.
Das im PatG statuierte Recht der Patientinnen und Patienten, die Patientendokumentation herauszuverlangen, wenn sie vom zuständigen Archiv nicht übernommen wird oder keine Anbietepflicht besteht, ist seit dem 15. Januar 2014 in Kraft. In der früher geltenden Fassung konnten die Patientinnen und Patienten die Patientendokumentation nach Ablauf der Aufbewahrungsfrist herausverlangen, sofern kein öffentliches Interesse an der weiteren Aufbewahrung bestand. Angesichts der geänderten Rechtslage besteht für die bisherige Auffassung, wonach die Patientinnen und Patienten auch während der Aufbewahrungsfrist Anspruch auf Herausgabe der Patientendokumentation im Original und unter Rückbehalt einer Kopie durch das Spital haben, kein Raum mehr.
In der Patientenbroschüre des Datenschutzbeauftragten, die 2013 neu erschienen ist und in einer zweiten, aktualisierten Auflage vorliegt, wurde diese Rechtsänderung berücksichtigt.

§§ 18 ff. PatG

05
Externe Kursleitende nicht unter Berufsgeheimnis

Ein privater Verein bietet fachliche Schulungen für Mitarbeitende im Pflegebereich an. Zur Vorbereitung einer Schulung soll die Kursleiterin jeweils mit Mitarbeitenden der Alters- oder Pflegeinstitution Gespräche führen sowie Einsicht in Pflegedokumentationen nehmen. Nach der Schulung soll ihre Wirkung wiederum anhand einer Einsichtnahme in die Pflegedokumentation evaluiert werden. Der Verein wandte sich mit der Frage an den Datenschutzbeauftragten, ob dieses Vorgehen zulässig sei.
Pflegedokumentationen von Institutionen wie Alters- und Pflegeheim sind Teil der Patientendossiers, gelten als besondere Personendaten und fallen unter das medizinische Berufsgeheimnis. Die Mitarbeitenden der Institution sind Hilfspersonen der Heimärztin bzw. des Heimarztes und haben die Schweigepflicht zu wahren. Es stellte sich die Frage, ob eine externe Kursleiterin ebenfalls als Hilfspersonen zu qualifizieren ist.
Als Hilfsperson gilt, wer bei der Berufstätigkeit des Geheimnisträgers in einer Weise mitwirkt, dass sie oder er grundsätzlich von den dabei wahrgenommenen Tatsachen Kenntnis erhält. Die Hilfsperson wird dann vom Berufsgeheimnis erfasst, wenn sie unter Leitung und Aufsicht des Geheimnisträgers tätig wird. Hilfspersonen des Arztes sind Assistentinnen und Assistenten, alle Mitarbeitenden im unter ärztlicher Leitung stehenden Team, Krankenpflegepersonal in Spitälern und Heimen usw. Im Vornherein ausgeschlossen ist die Qualifikation als Hilfsperson, wenn der Geheimnisträger gegenüber der Hilfsperson nicht weisungsbefugt ist.
Externe Kursleiterinnen und Kursleiter arbeiten nicht weisungsgebunden und sind auch nicht an der Behandlung bzw. Pflege beteiligt; sie fallen deshalb nicht unter den Begriff der Hilfsperson. Um eine Verletzung des Berufsgeheimnisses zu vermeiden, müssen die Alters- und Pflegeeinrichtungen, in denen die Schulungen stattfinden, die Patientendokumentationen entweder so weit anonymisieren, dass für die Kursleiterin keine Rückschlüsse auf die betroffenen Personen möglich sind, oder die Alters- und Pflegeeinrichtungen holen bei den betroffenen Patienten eine Einwilligung ein, dass die Kursleitung Einsicht in die Patientendokumentation nehmen darf. Der Datenschutzbeauftragte gab dem privaten Verein eine entsprechende Rechtsauskunft.

Art. 321 StGB

06
Einsatz von Kinderdiagnosetools

Ein öffentliches Organ wandte sich an den Datenschutzbeauftragten mit der Bitte, den Einsatz von Kinderdiagnosetools auf die datenschutzrechtlichen Anforderungen hin zu überprüfen. Bei den Tools handelt es sich um webbasierte Anwendungen, mit deren Hilfe die Lehrpersonen ihre Beobachtungen zu den einzelnen Kindern erfassen und auswerten können.
Zu prüfen war die Rechtmässigkeit der Datenbearbeitungen sowie die Voraussetzungen einer

Auslagerung, da die Anwendungen von Dritten angeboten werden. Was die Rechtmässigkeit der Datenbearbeitungen betrifft, finden sich die Rechtsgrundlagen im Volksschulgesetz (VSG) und in der Bildungsdatenverordnung. Im VSG werden die Beurteilung und Bewertung von Schülerinnen und Schülern sowie die Laufbahnentscheidungen geregelt. Es ist demnach Aufgabe der Lehrpersonen, die Lernenden anhand von Leistung, Lernentwicklung und Verhalten zu beurteilen. Die Bildungsdatenverordnung konkretisiert, welche Daten für die Aufgabenerfüllung benötigt werden. Darunter fallen auch Bewertungen sowie Stütz- und Fördermassnahmen. Der Datenschutzbeauftragte hat zudem die Verträge zwischen dem öffentlichen Organ und den Anbietern auf der Grundlage der rechtlichen Anforderungen und der «Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen» überprüft. Besonderes Augenmerk wurde dabei auf die Voraussetzungen für eine Auslagerung an Unterauftragnehmer im Ausland gelegt, da bei einem Anbieter Hosting und Support an zwei Unternehmen in Deutschland weiter ausgelagert worden waren.
Der Datenschutzbeauftragte wies darauf hin, dass Unterauftragnehmende sämtliche Verpflichtungen des Auftragnehmers übernehmen müssen. Besonders muss darauf geachtet werden, dass auch bei ausländischen Unterauftragnehmenden schweizerisches Recht zur Anwendung kommt und der Gerichtsstand in der Schweiz liegt. Weiter stellte der Datenschutzbeauftragte fest, dass in den Verträgen Bestimmungen über Vertragsdauer und -auflösung fehlten. Insbesondere fehlte die Bestimmung, dass im Auflösungsfall alle bearbeitenden Informationsbestände unentgeltlich an die Schulgemeinde zurück-übertragen werden müssen. Was die organisatorischen und technischen Anforderungen angeht, muss dem Umstand Rechnung getragen werden, dass besondere Personendaten betroffen sind. Unter anderem sind besondere Personendaten zu verschlüsseln und der Zugriff darf nur über eine qualifizierte Authentifizierung erfolgen.

§ 31 VSG
§ 32 VSG
§ 2 Abs. 1 Bildungsdatenverordnung
§ 6 IDG
§ 7 IDG
§ 22 IDV
§ 25 Abs. 2 IDV

07
Standardisiertes Abklärungsverfahren in der Schulpsychologie

Ein Schulpsychologischer Dienst wandte sich mit der Frage an den Datenschutzbeauftragten, ob das Volksschulamt dem Schulpsychologischen Dienst vorschreiben darf, künftig eine kantonale Datenbank für die schulpsychologischen Abklärungen zu verwenden. Es wurde befürchtet, das Volksschulamt erhalte durch den Betrieb der Datenbank Einsicht in sensitive Dossiers und würde die Daten zu eigenen Zwecken verwenden.
Der Kanton ist zuständig für das schulpsychologische Angebot und kann ein Klassifikationssystem zur schulpsychologischen Abklärung vorschreiben. Die Schulpsychologischen Dienste selbst werden jedoch von den Gemeinden getragen. Bis anhin wurden die sonderschulischen Abklärungen in einer Falldatenbank beim betreffenden schulpsychologischen Dienst geführt, wobei für das Abklärungsverfahren kein einheitlicher Standard bestand. Ab dem Schuljahr 2014/15 müssen nun alle Schulpsychologischen Dienste zur Abklärung sonderschulischer Massnahmen das elektronische Instrument «Standardisiertes

Abklärungsverfahren» (SAV-ZH) anwenden. Dieses dient dazu, die Abklärungen zu vereinheitlichen, was einen wesentlichen Beitrag zur Qualitätserfassung, zur Angebotsplanung und zum Controlling leistet. Im Rahmen dieses Verfahrens ist neu, dass das Volksschulamt eine Datenbank zur schulpsychologischen Abklärung zur Verfügung stellt und Daten (anonymisiert), die in die Datenbank einfliessen, auch zu eigenen Zwecken bearbeitet, wie beispielsweise zur Angebotsplanung.
Die Abklärungen ergaben namentlich Unklarheiten in Bezug auf die Verantwortung für die Datenbank und die Nutzung durch das Volksschulamt. Es wurde festgehalten, dass eine gesetzliche Grundlage für den Betrieb der Datenbank SAV-ZH ins Volksschulgesetz aufzunehmen ist, welche die Verantwortung für die Datenbank und auch die Nutzung der anonymisierten Daten durch das Volksschulamt regelt.

§ 19 Abs. 1 VSG
§ 36 Abs. 4 VSG
§ 38 Abs. 2 VSG
§ 5 Abs. 1 IDG
§ 8 IDG

08
Rahmenbedingungen für Online-Recherchen über Stellenbewerber

Heute besteht auch bei öffentlichen Organen die Versuchung, Stellenbewerberinnen und -bewerber zu «googeln», also im Internet Recherchen über die Kandidierenden anzustellen. Der Datenschutzbeauftragte publizierte deshalb ein Merkblatt, das Rahmenbedingungen und Grenzen von Online-Recherchen über Stellenbewerbende aufzeigt.
Im Auswahlverfahren ist in erster Linie von denjenigen Informationen auszugehen, die die Bewerberin oder der Bewerber einreicht (Lebenslauf, Arbeitszeugnisse, Aus- und Weiterbildungsnachweise usw.). Anlässlich des Vorstellungsgesprächs werden zusätzliche Informationen bei den Kandidatinnen und Kandidaten erfragt. Mit ihrer Zustimmung können auch Informationen bei Dritten (Referenzen) eingeholt oder Eignungstests durchgeführt werden. Dies alles ist für die betroffene Person transparent.
Bei Nachforschungen mittels Suchmaschinen (Google, Bing usw.) oder Personensuchdiensten wie Yasni resultieren unterschiedliche Ergebnisse. Berufliche und private Informationen können dabei nicht getrennt werden. Solche Recherchen greifen – soweit sie überhaupt zuverlässige Ergebnisse liefern – in die Privatsphäre der Bewerbenden ein und sind deshalb unzulässig. Gleiches gilt bei Recherchen oder gar Kontaktversuchen in privaten sozialen Netzwerken wie Facebook. Erlaubt ist dagegen die Beschaffung von Informationen aus beruflichen Netzwerken (wie Xing, Linkedin usw.). Persönliche Webseiten, Blogs und ähnliche Plattformen dürfen konsultiert werden, wenn in der Bewerbung ausdrücklich darauf hingewiesen wird.
In begründeten Ausnahmefällen ist es möglich, dass Informationen auch aus Suchdiensten oder privaten Netzwerken beschafft werden – jedoch nur wenn eine Funktion in einer besonderen Vertrauensstellung besetzt werden soll. Dazu sind folgende Voraussetzungen einzuhalten: Die Recherche ist auf Bewerbende zu begrenzen, die in die engere Auswahl kommen, vor der Recherche ist die Zustimmung einzuholen, die Ergebnisse sind kritisch zu prüfen und es ist der betroffenen Person Gelegenheit zur Stellungnahme zu den Ergebnissen zu geben.

§ 12 IDG
Personalgesetz

09
Überprüfung des Auskunftsrechts

Ein ehemaliger Mitarbeiter des Universitätsspitals Zürich (USZ) wandte sich an den Datenschutzbeauftragten, weil er vom USZ Auskunft über seine Personendaten verlangt und er keine vollständige Auskunft erhalten habe.
Bei der Überprüfung des Sachverhalts durch den Datenschutzbeauftragten zeigte sich, dass nebst dem Personaldossier über die Person noch Unterlagen aus ihrer Projekttätigkeit sowie eine Vielzahl weiterer Dokumente mit Personendaten vorhanden waren. Auch nach der Analyse der Unterlagen und nach Abklärungen beim USZ blieb für den Datenschutzbeauftragten vorerst unklar, ob das USZ das Auskunftsbegehren korrekt behandelt hatte. Das USZ vertrat die Meinung, seiner Auskunftspflicht nachgekommen zu sein. Aus den Akten ergaben sich jedoch Anhaltspunkte, wonach die betroffene Person in verschiedene Unterlagen keine oder keine vollständige Einsicht und dazu auch keine entsprechende Verfügung erhalten hatte. Aus diesem Grund führte der Datenschutzbeauftragte eine Kontrolle durch und nahm selbst Einsicht in die Akten.
Das USZ stellte die Akten zur Verfügung und erläuterte, in welche Dossiers es keine Einsicht gegeben hatte, weil sie seiner Meinung nach nicht unter das Auskunftsrecht fielen. Der Datenschutzbeauftragte qualifizierte in seinem Kontrollbericht die einzelnen Aktengruppen und gab Handlungsempfehlungen ab. Einzig die Akten aus der Projekttätigkeit fielen nicht unter das Auskunftsrecht. Hier ging es um die Frage, wem die Arbeitsergebnisse gehören – dem Mitarbeitenden oder der Institution – und somit um vertrags- und urheberrechtliche Fragen. Bei allen übrigen Akten bestand ein Auskunftsanspruch gemäss IDG. Falls es bei einzelnen Dossiers allenfalls überwiegende Interessen für Einschränkungen gab, waren diese nicht dem Auskunftsrecht zu entziehen, sondern es war eine anfechtbare Verfügung über die Einschränkung der Einsicht zu erlassen und der betroffenen Person der Rechtsweg zu ermöglichen. Das USZ ging entsprechend den Handlungsempfehlungen vor und erliess Verfügungen, soweit es die Einsicht einschränkte.

§ 20 Abs. 2 IDG
§ 23 IDG
§ 27 IDG

10
Personalsystem – noch nicht am PULS der Zeit

Nachdem der Regierungsrat 2009 beschlossen hatte, das Personalinformationssystem PALAS durch ein neues System zu ersetzen, führte das Personalamt per 1. Januar 2011 das neue Personal- und Lohnadministrationssystem (PULS) ein. Nebst reiner Personal- und Lohnadministration werden via PULS Rekrutierungen abgewickelt, Beurteilungen und Absenzen (auch gesundheitsbedingte) verwaltet oder Auswertungen gemacht. Im Vergleich zu den Vorgängersystemen hat die neue technische Lösung ein erheblich grösseres Potenzial für Persönlichkeitsverletzungen, weil immer mehr und auch immer mehr sensible Personendaten bearbeitet werden. Entsprechend müssen die Datenbearbeitungen gesetzlich ausreichend legitimiert sowie die technischen und organisatorischen Massnahmen nach dem aktuellen Stand der Technik getroffen und dokumentiert werden. Bereits 2009 hatte der Datenschutzbeauftragte auf den datenschutzrechtlichen Handlungsbedarf hingewiesen und die Schaffung von hinreichend bestimmten Rechtsgrundlagen im

Personalgesetz verlangt. Weiter forderte er in seinen Stellungnahmen mehrmals, dass ein Datenschutz- und Informationssicherheitskonzept sowie ein detailliertes Zugriffs- und Berechtigungskonzept zu erstellen seien. Es handelt sich bei diesen Konzepten um Basisdokumente zur Umsetzung der Anforderungen an die Informationssicherheit gemäss IDG respektive der Informatiksicherheitsverordnung (ISV).
Die Gesetzgebungsarbeiten kamen nur schleppend voran. Schliesslich wurde 2012 eine Vernehmlassung durchgeführt (siehe Tätigkeitsbericht 2012, Seite 37). Der Entwurf zur Änderung des Personalgesetzes war aus datenschutzrechtlicher Sicht zu begrüssen. Nach Abschluss der Vernehmlassung erfolgten jedoch aus gesetzgebungstechnischen Gründen nochmals grundlegende Anpassungen des Entwurfs, die dem Datenschutzbeauftragten wiederum vorgelegt wurden. Der neue, erheblich gekürzte und angepasste Entwurf des Personalamts genügte dem Transparenzgebot bzw. den Vorgaben des IDG gerade knapp und beseitigte Redundanzen zum IDG, weshalb der Datenschutzbeauftragte dem Entwurf zustimmte. Die Gesetzesvorlage an den Kantonsrat wurde Anfang 2014 verabschiedet.
Die Arbeiten am Datenschutz- und Informationssicherheitskonzept sowie am Zugriffs- und Berechtigungskonzept machten den Eindruck, als seien sie faktisch eingestellt worden. Obwohl der Datenschutzbeauftragte mehrmals und mit Nachdruck die Fertigstellung dieser grundlegenden Dokumente verlangte, lagen bis Ende 2013 nur unvollständige Entwürfe einzelner Dokumente vor. Von einer Dokumentation, wie sie nach bewährten Vorgehensweisen («best practice») bestehen müsste, ist PULS auch über drei Jahre nach Inbetriebnahme noch weit entfernt.
Die Möglichkeiten des Datenschutzbeauftragten, zur Behebung oder Verbesserung dieses Zustands beizutragen, sind erschöpft. Als letzte Einwirkungsbefugnis steht eine Kontrolle und in der Folge davon allenfalls die Anordnung von Massnahmen mittels förmlicher Empfehlung gemäss IDG offen.

§ 7 IDG
§ 8 Abs. 2 IDG
§§ 34 ff. Personalgesetz
§ 36 IDG

11
Medizinische Daten in der Konkursmasse

Ein Konkursamt war mit einem Gesuch um Herausgabe von Patientendaten eines Labors konfrontiert. Dabei wurde von den betroffenen Personen die Herausgabe der eigenen Krankenakte aus der Konkursmasse verlangt. Der zuständige Konkursbeamte wandte sich an den Datenschutzbeauftragten mit der Frage, ob die ersuchten Dokumente an die jeweilige betroffene Person herausgegeben werden dürfen. Zunächst war die Anwendbarkeit des IDG abzuklären. Beim zuständigen Konkursamt handelt es sich um ein öffentliches Organ, welches ein Zwangsvollstreckungsverfahren durchführt. Eröffnet wird das Verfahren durch eine richterliche Verfügung, durchgeführt wird es jeweils vom zuständigen Konkursamt, womit es unter den Anwendungsbereich des IDG fällt. Der Zugang zu den eigenen medizinischen Daten ist somit nach den Bestimmungen über das Auskunftsrecht nach IDG zu beurteilen. Hinzu kommt, dass nicht nur Auskunft, sondern die Herausgabe der Originalakten verlangt wurde. Als Bestandteil der Konkursmasse unterliegen die medizinischen Daten den Bestimmungen des Schuldbetreibungs- und Konkursrechts (SchKG). Demnach können Vermögenswerte zur Befriedung von Gläubigern verwertet werden. Die medizinischen Informationen werden aber durch das Berufsgeheimnis geschützt. Das ursprüngliche Vertragsverhältnis

zwischen den betroffenen Personen und dem konkursiten Labor war also von einer besonderen Geheimhaltungsvorschrift geprägt. Eine Verwertung und Bekanntgabe der durch das Berufsgeheimnis geschützten Daten ist somit nur mit der Einwilligung der betroffenen Personen möglich. Mit dem Gesuch um Herausgabe wird jedoch gerade der Wille manifestiert, dass die medizinischen Daten nicht verwertet werden sollen. Einer Herausgabe steht somit aus datenschutzrechtlicher Sicht nichts entgegen. Durch das Konkursamt zu prüfen sind noch allfällige Aufbewahrungspflichten, die einer Herausgabe entgegenstehen könnten.

§ 20 Abs. 2 IDG
Art. 221 SchKG
Art. 256 SchKG

12
Whistleblowing und Datenschutz

Die Frage der Zulässigkeit von Whistleblowing bei öffentlich-rechtlichen Institutionen (Kanton, Gemeinden etc.) wurde in der jüngsten Vergangenheit immer wieder in Medien und Öffentlichkeit diskutiert. Der Datenschutzbeauftragte hat dies zum Anlass genommen, aufzuzeigen, welche datenschutzrechtlichen Aspekte Angestellte bei der Offenlegung von Missständen beachten müssen.

Im personalrechtlichen Kontext umschreibt der Begriff Whistleblowing die Offenlegung von Missständen durch einen Angestellten gegenüber der Arbeitgeberin oder gegenüber externen Stellen wie zum Beispiel der Aufsichtsbehörde oder den Medien. Das Spektrum der Meldungen reicht von sexueller Belästigung über systematische Veruntreuung und Verstössen gegen Sicherheits- oder Umweltvorschriften bis hin zu Korruption.

Das Amtsgeheimnis verpflichtet die Angestellten zur Verschwiegenheit über dienstliche Angelegenheiten, soweit an der Geheimhaltung ein überwiegendes öffentliches oder privates Interesse besteht oder wenn eine besondere Vorschrift dies vorsieht. Ob Whistleblowing im Einzelfall gerechtfertigt ist, bestimmt sich somit wesentlich nach den auf dem Spiel stehenden Interessen.

Weiter verlangt das Prinzip der Verhältnismässigkeit, dass eine Meldung über Missstände zunächst auf dem Dienstweg erfolgt. Der Whistleblower darf Hierarchien überspringen, wenn Vorgesetzte selber in den Missstand involviert sind. Vom Dienstweg darf nur in Ausnahmefällen abgewichen werden, zum Beispiel wenn auch weitere Vorgesetzte oder die Aufsichtsbehörde selber in den Missstand involviert ist oder wenn Gefahr im Verzug ist. Kann der Dienstweg nicht eingehalten werden oder ergreift die Arbeitgeberin nach erfolgter Meldung keine wirksamen Massnahmen, ist zu prüfen, ob es geeignete Anlaufstellen ausserhalb der Anstellungsbehörde gibt. Im Kanton Zürich können Missstände dem Ombudsmann gemeldet werden.

Der Weg an die Öffentlichkeit ist nur in Ausnahmefällen zulässig. Der Verhältnismässigkeitsgrundsatz fordert, dass die in der Öffentlichkeit aufgezeigten Missstände ein gewisses Gewicht haben. Zudem muss der Whistleblower die Meldung in guten Treuen anbringen und im Interesse der Öffentlichkeit, des Arbeitgebers oder im Interesse von Personen handeln, die vom Arbeitgeber nicht ordnungsgemäss behandelt werden.

Schliesslich muss der Whistleblower – soweit es die Umstände erlauben – auch selbst sorgfältig prüfen, ob die Informationen zutreffend und zuverlässig sind: Ein Angestellter darf nicht leichtfertig falsche oder ungesicherte Tatsachen melden.

Art. 16 Abs. 2 BV
§ 49 Personalgesetz
§ 51 Personalgesetz
Art. 320 StGB
§ 23 IDG

13
Verkehrsmonitoring mittels Überwachung

Das Verkehrsmonitoring zur Analyse von Verkehrsströmen und -verhalten sowie zur Messung der Effektivität von Verkehrssteuerungsmassnahmen erfreut sich zunehmender Beliebtheit. Die Bandbreite der Methoden ist gross und reicht von einfachen Zählkästen am Strassenrand über GPS-basierte Verkehrsflussbeobachtungen bis hin zu Videoüberwachungsmassnahmen. Verschiedene Ingenieurbüros, die im Auftrag von öffentlichen Organen solche Verkehrsmonitorings durchführten, ersuchten den Datenschutzbeauftragten um eine Beurteilung ihrer Projekte.
In den zu beurteilenden Fällen ging es jeweils um ein Verkehrsmonitoring anhand von Videobeobachtungen. Während zwei Projekte zum Ziel hatten, die Sicherheit von Verkehrsteilnehmenden durch die Einführung technischer Massnahmen zu verbessern, verfolgte das dritte Projekt den Zweck, den Verkehrsfluss zu verbessern. Die drei Projekte hatten gemeinsam, dass bestimmte Strassenabschnitte über einen gewissen Zeitraum mittels Videokameras überwacht und die Aufzeichnungen anschliessend dem jeweiligen Zweck entsprechend ausgewertet werden sollten.
Bei Videoüberwachungen im Rahmen von Verkehrsmonitorings ist zentral, dass Art der Überwachung, räumliche und zeitliche Ausdehnung sowie Aufbewahrungsdauer und Löschfristen verhältnismässig sind. Wichtig ist weiter, dass die Aufnahmen nicht zu anderen Zwecken verwendet werden und die Videoüberwachung für betroffene Personen erkennbar ist. Ausschnitt und Auflösung der Kameras sind so zu wählen, dass möglichst keine Personen und keine privaten Wohnbereiche (Fenster, Balkone, Gärten usw.) im Bildausschnitt zu erkennen sind. Zeitlich ist der Betrieb auf die für die verfolgten Ziele relevanten Tagesabschnitte zu beschränken. Aus Transparenzgründen ist ein Reglement über die Videoüberwachung zu erlassen.
Die dem Datenschutzbeauftragten vorgelegten Projekte erfüllten die genannten Anforderungen weitestgehend. Soweit Anpassungsbedarf bestand, wurden die notwendigen Änderungen von den Projektverantwortlichen umgesetzt.

§ 8 Abs. 1 IDG
§ 14 Strassengesetz (StrG)

14
Regeln für Bedrohungsmanagement

Um Drohungen, Belästigungen oder eine mögliche Gewaltanwendung gegenüber Mitarbeitenden, Kundinnen und Kunden frühzeitig zu erkennen und, wo angezeigt, deeskalierend einzugreifen, plante das Universitätsspital Zürich (USZ), ein so genanntes Bedrohungsmanagement einzurichten. Da ein solches Instrument meist auch eine Bearbeitung und einen Austausch von Personendaten beinhaltet, gelangte das USZ mit einem Entwurf an den Datenschutzbeauftragten.
Anlässlich einer vom Datenschutzbeauftragten einberufenen Sitzung wurde das Konzept mit Vertretern des USZ im Detail besprochen. Dabei zeigte sich, dass die geplanten Abläufe, die Organisationsform und die damit verbundenen Datenbearbeitungen verhältnismässig ausgestaltet werden sollten. Notwendig war jedoch die Schaffung einer Rechtsgrundlage, damit die Datenbearbeitungen über die betroffenen Mitarbeitenden legitimiert waren. Der Datenschutzbeauftragte empfahl dem USZ deshalb den Erlass eines Reglements. Das USZ legte dem Datenschutzbeauftragten den Entwurf der Regelung zur Stellungnahme vor und nahm dessen Hinweise in die definitive Fassung auf.

Vernehmlassungen

«In der Gesetzgebung werden wichtige Weichen für einen wirksamen Schutz der persönlichen Freiheit der Bürgerinnen und Bürger gestellt.»

Wahrung der Verhältnismässigkeit

In zahlreichen Gesetzgebungsverfahren hat der Datenschutzbeauftragte auf einen wirksamen Schutz der persönlichen Freiheit der Bürgerinnen und Bürger bei zunehmenden Datenbearbeitungen hingewiesen.

Viele Gesetzesänderungen betrafen den Polizei- und Sicherheitsbereich (Seiten 37 bis 39). In den Bereichen Polizei, Migration, Asyl, Staatsschutz, Fernmeldeüberwachung usw. werden die Befugnisse für Datenbearbeitungen und die Zugriffsrechte von Sicherheitsbehörden auf Datenbanken aus anderen Vollzugsbereichen laufend erweitert. Selbst wenn sich die Änderungen im Einzelfall mit einem öffentlichen (Sicherheits-)Interesse rechtfertigen lassen, erregt die allgemeine Tendenz Besorgnis. Die Parlamente sind verstärkt gefordert, die Balance von Freiheit und Sicherheit in einer Gesamtsicht zu wahren.

Sensible Datenbearbeitungen

Die Übergangsfrist gemäss § 41 IDG ist am 30. September 2013 abgelaufen. § 41 IDG verlangt, dass für sensible Datenbearbeitungen innert fünf Jahren nach Inkrafttreten des IDG hinreichend bestimmte Regelungen in formellen Gesetzen zu schaffen sind. Es stimmt nachdenklich, dass diese grosszügige Übergangsfrist nur vereinzelt eingehalten wurde; in vielen Bereichen fehlen nach wie vor entsprechende Rechtsgrundlagen. Nur die Bildungsdirektion (siehe Tätigkeitsbericht 2012, Seite 36) und die Direktion der Justiz und des Innern haben umfassende Gesetzesanalysen durchgeführt und entsprechende Gesamtvorlagen vorbereitet (siehe auch Seite 39).

Zwei Änderungen des IDG betreffen den Datenschutzbeauftragten, der neu vom Kantonsrat gewählt wird, und eine weitere Revisionsvorlage nimmt den Kantonsrat und seine Aufsichtskommissionen teilweise vom Geltungsbereich des IDG aus (siehe Seite 40).

Erwähnenswert ist zudem, dass sich der Bund mit einer Revision des Datenschutzgesetzes (DSG) befasst und dabei die Option einer gesamtschweizerischen Vereinheitlichung des Datenschutzrechts prüft. Der Kanton Zürich nahm zuhanden der Konferenz der Kantonsregierungen Stellung. Der Datenschutzbeauftragte erachtet diesen Weg als gangbar, sofern das DSG klar zwischen öffentlich-rechtlichen und privatrechtlichen Datenbearbeitungen unterscheidet, das Gesetz unter Einbezug der Kantone neu konzipiert wird sowie Aufsicht und Rechtsschutz im kantonalen und kommunalen öffentlich-rechtlichen Bereich bei den Kantonen verbleiben.

Der Datenschutzbeauftragte hat 2013 unter anderem zu folgenden Gesetzgebungsprojekten Stellung bezogen:

Kanton

- Änderung des Einführungsgesetzes zum Kindes- und Erwachsenenschutzrecht (EG KESR)
- Änderung des IDG und des Kantonsratsgesetzes
- Änderung der Verordnung über das Polizei-Informationssystem POLIS
- Teilrevision der Bürgerrechtsverordnung
- Gesetz über die in der Direktion der Justiz und des Innern verwendeten besonderen Personendaten
- Gesetz über die Administrativuntersuchung
- Totalrevision Publikationsgesetz
- Neuerlass einer kantonalen Lebensmittel- und Gebrauchsgegenständeverordnung
- Totalrevision der Tierseuchenverordnung

Bund

- Neuerlass eines Bundesgesetzes über den zivilen Nachrichtendienst
- Übernahme und Umsetzung der Verordnungen (EU) Nr. 604/2013 (Dublin-III-Verordnung) und (EU) Nr. 603/2013 (Eurodac-Verordnung); Weiterentwicklungen des Dublin/Eurodac-Besitzstands
- Übernahme der EU-Verordnung betreffend Einführung eines Europäischen Überwachungssystems (EUROSUR)
- Übernahme der EU-Verordnung betreffend Einführung eines Evaluierungsmechanismus für die Prüfung der Anwendung des Schengen-Besitzstands
- Übernahme der EU-Verordnung zur Änderung des Schengener Grenzkodex sowie weiteren Änderungen im Ausländer- und Asylrecht
- Bundesgesetz über Verbesserungen beim Informationsaustausch zwischen Behörden im Umgang mit Waffen
- Teilrevision der Statistikerhebungsverordnung und Neuerlass einer Verordnung über die Datenverknüpfung
- Änderung des Obligationenrechts (Handelsregisterrecht, Akten-, GmbH- und Genossenschaftsrecht) und des Revisionsaufsichtsrechts
- Bundesgesetz über die Registrierung von Krebskrankheiten

Nachrichtendienst auf neuer Gesetzesgrundlage

Mit dem Nachrichtendienstgesetz wird eine einheitliche formellgesetzliche Grundlage auf Stufe Bund geschaffen, die den Organen des Nachrichtendienstes weitgehende Kompetenzen zur Informationsbeschaffung einräumt. Das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und das Bundesgesetz über die Zuständigkeit im Bereich des zivilen Nachrichtendienstes werden aufgehoben.

Neu sollen den Organen des Nachrichtendienstes dieselben, mitunter sogar weiter gehende Beschaffungsmassnahmen zur Verfügung stehen als den Strafverfolgungsbehörden im Rahmen eines gerichtspolizeilichen Ermittlungsverfahrens. Es soll auch Government-Software präventiv im Staatsschutzbereich eingesetzt werden können. Bei Letzterem handelt es sich um das Eindringen in Computersysteme und -netzwerke unter Zuhilfenahme technischer Geräte, um dort vorhandene Informationen zu beschaffen sowie den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Anders als in der Schweizerischen Strafprozessordnung beschränken sich die staatsschutzrechtlichen Mittel also nicht auf die reine Überwachung. Abgesehen von den in der Praxis schwierigen Abgrenzungsfragen zu kriminalpolizeilichen Verfahren stellt sich die Frage der Verhältnismässigkeit von Massnahmen mit derart drastischen Eingriffen in die persönliche Freiheit und die informationelle Selbstbestimmung.

Persönliche Freiheit muss gewahrt bleiben

Wenn solche Instrumente überhaupt eingesetzt werden sollen, sind die Rahmenbedingungen so zu schaffen, dass Rechtssicherheit besteht und der Kernbereich der Freiheitsrechte nicht tangiert wird. Die Bestimmungen müssen somit hinreichend bestimmt, die Genehmigungen durch unabhängige Kontrollorgane vorgenommen und nach Abschluss auf ihre Verhältnismässigkeit überprüft werden. Weiter sind die Rechte betroffener Personen uneingeschränkt zu wahren. Im Gesetzesentwurf wird keine explizite Beschwerdemöglichkeit statuiert und der Genehmigungsprozess sieht auch keine vorgängige Beschränkung respektive Nennung der expliziten Datentypen vor. Es sollte daher eine kompetente Stelle mit der Auswertung solcher Einsätze beauftragt werden: Jeder Einsatz sollte nachträglich auf seine Verhältnismässigkeit und das Einhalten der Rahmenbedingungen überprüft werden. Insbesondere darf nicht in den Kernbereich der Freiheitsrechte eingegriffen werden. Zudem hat jeder Eingriff im Rahmen von sicherheitspolitisch relevanten Bedrohungen zu erfolgen, in dem gemäss dem Bericht zum Vorentwurf keine strafrechtlichen Ermittlungen stattfinden dürfen.
Das Gesetz erklärt das Datenschutzrecht des Bundes für anwendbar. Dabei wurde allerdings vernachlässigt, dass bei der Bestimmung des anwendbaren Datenschutzrechts auf das Organ abgestützt, welches die Daten bearbeitet und somit bis zur Einspeisung der Daten in die Bundessysteme die kantonalen Datenschutzgesetze zur Anwendung kommen. Auch was die Kontrolle betrifft, lässt die Vorlage die Tatsache der Kontroll- und Aufsichtstätigkeit der kantonalen Datenschutzbehörden ausser Acht.

Revision der POLIS-Verordnung

Die Änderungen des Polizeigesetzes sind am 1. Mai 2013 in Kraft getreten. Unter anderem wurden die Bestimmungen über den Datenschutz vereinheitlicht und eine Rechtsgrundlage für eine verdachtsunabhängige, systematische und automatisierte Überprüfung aller Hotelgäste geschaffen. Diese Änderungen bedingten wiederum eine Anpassung der POLIS-Verordnung.

Der Datenschutzbeauftragte begrüsste grundsätzlich die Zusammenführung der datenschutzrechtlichen Bestimmungen auf formellgesetzlicher Grundlage. Im Zentrum seiner Kritik stand aber bereits bei der Vernehmlassung zur Revision des Polizeigesetzes die Einführung der verdachtsunabhängigen, systematischen und automatisierten Überprüfung aller Hotelgäste. Dieselben Bedenken gelten nun auch für die entsprechenden Bestimmungen in der POLIS-Verordnung. So ist aus datenschutzrechtlicher Sicht eine solche Kontrolle nicht nur unverhältnismässig, sondern verstösst auch gegen die Bestimmungen des für die Schweiz geltenden Schengener Durchführungsübereinkommens, welches nur die einzelfallweise Überprüfung ausländischer Staatsangehöriger zum Zweck der Gefahrenabwehr und der Strafverfolgung erlaubt. Die durch diesen Prozess bearbeiteten Informationen sind, obwohl per se nicht als sensibel eingestuft, als besondere Personendaten zu qualifizieren, da sie durch Strafverfolgungsbehörden zum Zweck der Strafverfolgung bearbeitet werden. Da auch Daten von unbescholtenen Bürgerinnen und Bürgern bearbeitet und für drei Jahre in der Datenbank POLIS gespeichert werden, hat der Datenschutzbeauftragte gefordert, die zu erfassenden Daten strikt auf die für eine eindeutige Identifizierung der Personen notwendigen Kategorien zu beschränken.

Zwingende Löschung von «No-Hits»

Was die Aufbewahrungsfrist von drei Jahren sowohl der Hits als auch der No-Hits betrifft, so ist mit Blick auf das Verhältnismässigkeitsprinzip festzuhalten, dass das Aufbewahren der No-Hits während dieser für diese Datenkategorie relativ langen Dauer unverhältnismässig ist. Daten dürfen so lange aufbewahrt werden, wie sie für die Aufgabenerfüllung benötigt werden. No-Hits müssten folglich nach dem Abgleich mit den polizeilichen Informationssystemen sofort gelöscht werden.

Übernahme und Umsetzung von Dublin-III- und Eurodac-Verordnungen

Die Dublin-III- und die Eurodac-Verordung sind Neufassungen auf EU-Ebene auf der Basis des Dublin/Eurodac-Besitzstands. Diese sind innert zweier Jahre durch die Schweiz zu übernehmen. Da Erstere in der EU bereits in Kraft ist, werden die direkt anwendbaren Bestimmungen auch in der Schweiz ab dem 1. Januar 2014 vorläufig angewendet. Die heutigen Gesetzesbestimmungen entsprechen zum grössten Teil den auf der EU-Ebene verabschiedeten Neuerungen. Anpassungen sind nur punktuell im Bundesgesetz über die Ausländerinnen und Ausländer sowie im Asylgesetz notwendig.
Namentlich die neuen Bestimmungen in der Eurodac-Verordnung gaben Anlass zu datenschutzrechtlicher Kritik. Als Beispiel ist der neu durch die Strafverfolgungsbehörden mögliche Zugriff auf die Fingerabdruckdaten zu erwähnen. Festzuhalten ist, dass dieser zum heutigen Zeitpunkt zwar nicht zur Weiterentwicklung des Dublin/Eurodac-Besitzstands zählt, dass aber anzunehmen ist, dass sich dies in näherer Zukunft ändern wird.
Diese Zugriffe stellen nicht nur einen tiefen Eingriff in die Persönlichkeitsrechte Betroffener, sondern auch eine Zweckänderung der ursprünglich mit Blick auf die Prüfung des Erstasylgesuchs erfassten Daten dar. Alle Asylsuchenden werden einem Generalverdacht unterstellt. Allein die Tatsache, dass die Daten für die Strafverfolgung geeignet sind, kann eine solche Zweckänderung nicht rechtfertigen, denn sie würde einer Verhältnismässigkeitsprüfung nicht stand halten.

Besondere Personendaten in der Justizdirektion

Die Direktion der Justiz und des Innern (JI) schickte eine umfassende Vorlage zur Anpassung der Rechtsgrundlagen der einzelnen Fachbereiche der JI an die Anforderungen des IDG in die Vernehmlassung. Gemäss §§ 8 Abs. 2 und 17 Abs. 1 lit. a IDG bedarf das Bearbeiten bzw. Bekanntgeben besonderer Personendaten einer hinreichend bestimmten Regelung in einem formellen Gesetz.
Bezüglich Abrufverfahren, Datenaufbewahrung, Akteneinsicht sowie zentrale Aufbewahrung und Verwertung von Beweismitteln, beschlagnahmten Gegenständen und Vermögenswerten war Anpassungsbedarf festgestellt worden, und es wurden Teilrevisionen des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess, des Straf- und Justizvollzugsgesetzes sowie des Einführungsgesetzes zum Opferhilfegesetz ausgearbeitet. Der Datenschutzbeauftragte brachte verschiedene Hinweise an, beispielsweise betreffend das Akteneinsichtsrecht der Parteien in Akten abgeschlossener Verfahren, die Aufbewahrungsfristen von Strafakten sowie die Einsichtnahme in Patientendokumentationen von im Straf- oder Massnahmenvollzug befindlichen Personen durch ärztliche Mitarbeitende der für den Justizvollzug zuständigen Amtsstelle und in ihrem Auftrag tätige Ärztinnen und Ärzte. Die JI nahm die Hinweise mehrheitlich auf. Die Vorlage wurde im Herbst 2013 vom Regierungsrat zuhanden des Kantonsrats verabschiedet.

Anpassungen des IDG

Anpassungen des IDG führten einerseits zu einer Betonung der institutionellen Unabhängigkeit des Datenschutzbeauftragten. Andererseits wurden der Kantonsrat und seine Aufsichtskommissionen teilweise vom Geltungsbereich des IDG ausgenommen.

Unter dem Titel «Effizienzsteigerung» revidierte der Kantonsrat das Kantonsratsgesetz und sein Geschäftsreglement. Dabei wurde das Wahlverfahren für den Datenschutzbeauftragten geändert. Bisher wählte der Regierungsrat den Datenschutzbeauftragten und die Wahl bedurfte der Genehmigung durch den Kantonsrat. Künftig wählt der Kantonsrat den Datenschutzbeauftragten auf Vorschlag des Regierungsrates.
In der Vernehmlassung hatte der Datenschutzbeauftragte darauf hingewiesen, dass weiterer Handlungsbedarf besteht, wie zum Beispiel die Regelung von Pilotprojekten für Datenbearbeitungen und Datenplattformen sowie die interinstitutionelle Zusammenarbeit, und vorgeschlagen, die Änderungen im Rahmen einer grösseren Teilrevision des IDG zu planen. Der Kantonsrat änderte das IDG im Rahmen der Vorlage zur Effizienzsteigerung lediglich im erwähnten Punkt.
Insgesamt ist diese Anpassung zu begrüssen, da sie die institutionelle Unabhängigkeit des Datenschutzbeauftragten stärkt. Sie hat auch Auswirkungen auf die Berichterstattung. Der Datenschutzbeauftragte berichtet dem Wahlorgan, weshalb der Kantonsrat neu Hauptadressat des Tätigkeitsberichts ist.

Kommissionsmotion mit weit reichenden Folgen

Eine weitere Änderung des IDG wurde durch eine Motion der Kommission Aufsicht und Bildung des Kantonsrats (KR-Nr. 236/2012) ausgelöst. In Umsetzung der Motion soll eine Ausnahme des Geltungsbereichs des IDG für den Kantonsrat und seine Kommissionen vorgesehen werden. Der Datenschutzbeauftragte nahm zu diesem Vorschlag Stellung: Eine solche Ausnahme ist aus verfassungsrechtlicher Sicht nur opportun, wenn andernorts detaillierte Regelungen über die Datenbearbeitungen bestehen. Dies ist zum Beispiel für Gerichtsverfahren (Zivilprozessordnung, Strafprozessordnung usw.) oder bei den öffentlichen Registern des Privatrechts (Grundbuch, Handelsregister usw.) der Fall. Die Geschäftsleitung nahm die Einwände weitgehend auf, begrenzte die Ausnahme auf bestimmte Aspekte der Oberaufsicht und sah gleichzeitig eine Konkretisierung dazu im Kantonsratsgesetz vor.

§ 30 IDG
§ 2 IDG
§§ 34e, 34f, 43 KRG

Vorabkontrollen bei E-Government

Anlässlich der Erneuerung der E-Government-Strategie des Regierungsrates wurde auch der Datenschutzbeauftragte zur Vernehmlassung zu Strategie und Umsetzungsplan 2013–2016 eingeladen. Die verstärkte übergreifende Steuerung und Koordination von E-Government durch die Staatskanzlei wurde begrüsst, da in der neuen Strategie auch einige Querschnittprojekte geplant sind. Datenschutzrechtlicher Handlungsbedarf besteht bei folgenden Zielen und Handlungsschwerpunkten von E-Government: Für die Mehrfachnutzung von Daten im Rahmen von E-Government und für den Aufbau zentraler Informatikinfrastrukturen (wie zentrale Identity-Verwaltung und digitale Signaturen) sind Rechtsgrundlagen zu schaffen. Auch bei so genannten «Open Government Data» sind die Rahmenbedingungen des Datenschutzes zu beachten; vermeintlich anonyme Daten können durch Kombinationen rasch einen Personenbezug erhalten und entsprechend sensibel werden. Ein Einbezug des Datenschutzbeauftragten in die ständige E-Government-Organisation wurde nicht vorgesehen, was vertretbar ist, weil die massgeblichen Projekte ohnehin im Rahmen einer Vorabkontrolle datenschutzrechtlich zu prüfen sind.

Registrierung von Krebserkrankungen

Mit dem Erlass eines neuen Bundesgesetzes über die Registrierung von Krebserkrankungen sollen diese flächendeckend einheitlich und vollständig erfasst werden, um Aussagen über ihre Häufigkeit und den Verlauf machen zu können und eine Grundlage für Prävention, Früherkennung und Behandlung von Krebserkrankungen zu schaffen. Der Datenschutzbeauftragte begrüsste in der Vernehmlassung die Schaffung bundesrechtlicher Vorschriften über die Registrierung von Krebserkrankungen (siehe auch Tätigkeitsbericht 2011, Seite 35). Das Bestreben, dem Schutz der Persönlichkeit der Patientinnen und Patienten Rechnung zu tragen, war im Vorentwurf klar erkennbar. Allerdings waren verschiedene Prozesse nicht zu Ende gedacht und warfen Fragen auf, beispielsweise die anonymisierte Übermittlung des Widerspruchs der Patientin oder des Patienten in Fällen, in welchen die Daten bereits übermittelt wurden. Der Datenschutzbeauftragte kritisierte überdies wegen fehlender Verhältnismässigkeit diverse Bestimmungen, etwa die Verwendung der Versichertennummer der AHV (AHVN13) als Personenidentifikator sowie den Abgleich der Daten mit den kantonalen und kommunalen Einwohnerregistern und mit der Todesursachenstatistik des Bundesamts für Statistik. Sodann regte er die Aufnahme einer Bestimmung betreffend die Informationssicherheit an, da dem Schutz der Daten durch technische und organisatorische Massnahmen hohes Gewicht beizumessen ist.

Handelsregister

Das Eidgenössische Justiz- und Polizeidepartement gab einen Vorentwurf zur Änderung des Obligationenrechts (Handelsregisterrecht sowie Anpassungen im Aktien-, GmbH- und Genossenschaftsrecht) und des Revisionsaufsichtsrechts in die Vernehmlassung. Eine zentrale Änderung betraf den Aufbau einer nationalen Infrastruktur des Handelsregisters durch den Bund; für die Führung des Handelsregisters bleiben die Kantone zuständig.
Der Datenschutzbeauftragte wies in seiner Stellungnahme darauf hin, dass aus dem Vorentwurf nicht klar ersichtlich ist, dass es sich beim Handelsregister um ein vollständig elektronisch geführtes Register handelt. Sodann sind der Zweck und der Umfang des Personenregisters unklar, welches eingeführt werden soll. Das Transparenzgebot verlangt, dass der Einzelne erkennen kann, zu welchem Zweck welche Daten über ihn bearbeitet werden. Weiter sprach sich der Datenschutzbeauftragte gegen die Verwendung der Versichertennummer der AHV (AHVN13) als Personenidentifikator aus, zumindest so lange, bis eine grundlegende Diskussion über die Vor- und Nachteile deren Verwendung geführt und allenfalls ein Grundsatzentscheid für die Verwendung mit klaren Voraussetzungen und strikten Rahmenbedingungen auf Gesetzesstufe verankert worden ist. Schliesslich begrüsste der Datenschutzbeauftragte die Regelung, dass die im Internet veröffentlichten Daten zehn Jahre nach der Löschung der Rechtseinheit nicht mehr zugänglich sind, empfahl aber, eine kürzere Frist vorzusehen. Zudem sollte der betroffenen Person bei überwiegendem Interesse ein Recht auf Löschung der Daten eingeräumt werden.

Mangelhafte Regelungen in der Bundesstatistik

Das Eidgenössische Departement des Innern führte eine Vernehmlassung zur Teilrevision der Statistikerhebungsverordnung und zum Neuerlass einer Datenverknüpfungsverordnung durch. Der Datenschutzbeauftragte nahm kantonsintern im Mitberichtsverfahren dazu Stellung. Zu bemängeln war in erster Linie die für die vorgesehenen Datenverknüpfungen ungenügende Grundlage auf Gesetzesstufe (Delegationsnorm). Weiter war die Verwendung der AHVN13-Nummer für die Verknüpfungen vorgesehen; hier war ein weiteres Mal (siehe Tätigkeitsbericht 2012, Seite 34) zu beanstanden, dass diese personalisierte, sozialversicherungsrechtlichen Zwecken dienende Nummer anderen Zwecken dienen soll. Gerade im Statistikbereich ist die Verwendung eines Personenidentifikators (statt eines vollständig anonymen Codes) verheerend und entzieht der Statistik die Berechtigung für eine datenschutzrechtliche Privilegierung. Darüber hinaus waren weitere Regelungen zu bemängeln, die nur vermeintlich zu Rechtssicherheit und Transparenz beitragen. Auch die Vereinigung der Schweizerischen Datenschutzbeauftragten (privatim) wies auf diese gravierenden Mängel hin. Dennoch wurden die Verordnungen praktisch unverändert in Kraft gesetzt.

«Strukturierte Vorlagen und Anleitungen helfen, das Niveau der Informationssicherheit zu verbessern.»

Grosse Unterschiede in der Umsetzung

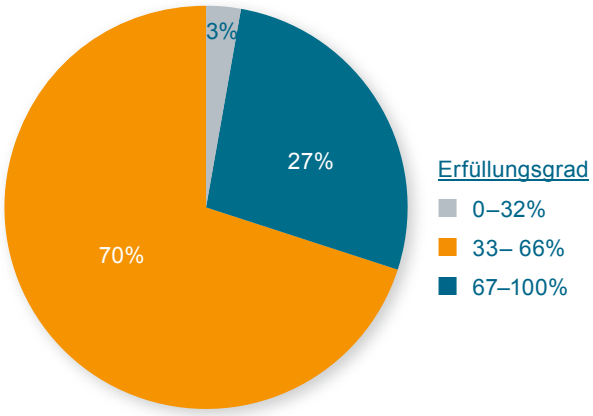
Mit Anleitungen zur Umsetzung der vom IDG verlangten Sicherheitsmassnahmen kann generell eine Verbesserung erzielt werden. Dennoch bleibt der Umsetzungsgrad bei den einzelnen öffentlichen Organen sehr unterschiedlich.

Die Mustervorlagen des Datenschutzbeauftragten, welche basierend auf den Standards des deutschen Bundesamts für Sicherheit in der Informatiktechnik (BSI) an die Bedürfnisse der Gemeinden und Schulen im Kanton Zürich angepasst wurden, haben sich in der Praxis bewährt. So ist der Umsetzungsgrad der gesetzlich geforderten Massnahmen zur Informationssicherheit merklich gestiegen. Es konnte festgestellt werden, dass die kontrollierten Stellen im Bereich Informationssicherheit vergleichbare Schwerpunkte setzten, und zwar unabhängig davon, wie gross die geprüfte Stelle respektive die Anzahl der von den Datenbearbeitungen betroffenen Personen war. Zu erwähnen sind namentlich der Bereich Inter- und Intranet sowie die Anstrengungen bei Zugriffsverwaltung, Identifizierung und Authentisierung. Beim erreichten Umsetzungsgrad zeigten sich hingegen grosse Differenzen. So wurde klar ersichtlich, dass dort, wo sich Spezialisten dieser Aufgabe widmen konnten, auch mehr Informationssicherheit erreicht wurde.

Als neues Instrument kam 2013 ein Webscanner zum Einsatz. Mit dem Webscanner können auf einfache Weise Schwachstellen bei den Webanwendungen aufgezeigt werden. Bei 179 geprüften Anwendungen wurden 27 kritische Schwachstellen entdeckt, die es zu beheben galt.

Weiter hat der Datenschutzbeauftragte in einer erweiterten Datenschutz-Review neben den organisatorischen und technischen Massnahmen auch eine vertiefte rechtliche Prüfung vorgenommen. Dabei wurde ein kompletter Datenbearbeitungsprozess mit Blick auf die Umsetzung der gesetzlichen Bestimmungen überprüft, und zwar in einem Bereich, in dem fast ausschliesslich besondere Personendaten bearbeitet werden.

Erfüllungsgrad aller geprüften Stellen 2011–2013



Komplexe IT-Infrastrukturen schützen

Kontrollen im Schulbereich haben gezeigt, dass bei komplexen IT-Strukturen ein grösserer Aufwand für die Sicherheit notwendig ist.

Der Datenschutzbeauftragte hat acht Berufs- und Mittelschulen kontrolliert. Dabei wurden diverse rechtliche Aspekte sowie solche der Informationssicherheit anhand einer umfassenden Analyse überprüft. Das Resultat zeigte, dass bei den Schulen oft dieselben Schwachstellen existieren.

Vielfach fehlte ein Sicherheitskonzept; also ein Dokument, das definiert, wo die sensitiven personenbezogenen Daten gespeichert sind und wie diese geschützt werden. Ohne eine solche Definition ist es schwierig, einen adäquaten Schutz zu gewährleisten. Weiter wurden die Mitarbeitenden kaum im Bereich der Informationssicherheit und des Datenschutzes sensibilisiert, obwohl im Schulumfeld zunehmend Webdienste verwendet werden. Da gerade das menschliche Verhalten eines der grössten Risiken im Bereich der Informationssicherheit darstellt, sollte diesem Punkt vermehrt Beachtung geschenkt werden. Weitere Mängel waren unsichere Passwörter, fehlende oder unzureichende Weisungen für die Mitarbeitenden, ein schwacher Schutz der Daten auf mobilen Geräten (insbesondere Smartphones) und fehlende Datenschutzbestimmungen in den Verträgen mit den Lieferanten.

Bei einer Berufsschule wurde auf der Website eine schwerwiegende Sicherheitslücke aufgedeckt. Dadurch war es via Internet möglich, auf alle Daten des Schulnetzes zuzugreifen, ohne sich vorgängig authentifizieren zu müssen.

Der Datenschutzbeauftragte begleitet zurzeit ein Informationssicherheitsprojekt mit dem Mittelschul- und Berufsbildungsamt, um möglichst praxisnahe Vorlagen und Hilfestellungen für die Schulen zu erarbeiten, welche sich mit geringem Aufwand an die Gegebenheiten der jeweiligen Bildungsinstitution anpassen lassen. Ziel ist es, dass jede Schule mit angemessenem Aufwand einen grösstmöglichen Schutz für die Daten gewährleisten kann.

Kurse für Informationssicherheit im Gemeinde- und Spitex-Umfeld

Mitarbeitende von kleineren Gemeinden hatten die Möglichkeit, an Kursen Wissen zu erwerben, wie ihre Daten gesetzeskonform geschützt werden können. Dazu wurden vier halbtägige Kurse durchgeführt.

Aufgrund der Resultate der Datenschutz-Reviews hat der Datenschutzbeauftragte in den letzten Jahren Dokumente und Vorlagen zur Verfügung gestellt, die von den Gemeinden für den Aufbau und die Etablierung ihres Sicherheitsprozesses genutzt werden können. Die Unterlagen wurden speziell an die Bedürfnisse von Gemeinden mit weniger als 4000 Einwohnerinnen und Einwohnern angepasst. Der Inhalt wurde im Rahmen von Schulungen vermittelt. Durch die Kurse sollten die Teilnehmenden den Ablauf des Sicherheitsprozesses verstehen und befähigt werden, die Dokumente und Vorlagen so zu nutzen, dass sie am Arbeitsplatz ohne grossen Aufwand eingesetzt werden können. Der Kurs richtete sich vor allem an die IT- respektive Informationssicherheitsverantwortlichen kleiner Gemeinden, wurde jedoch auch für Spitex-Organisationen ausgeschrieben, die hinsichtlich Grösse und Komplexität im Bereich Datenbearbeitung den kleineren Gemeinden sehr ähnlich sind.

Die Lernziele des Kurses waren wie folgt definiert:

- Die Teilnehmenden kennen die Vorlagen, Anleitungen, Beispiele und Checklisten für die Informationssicherheit.
- Die Teilnehmenden verstehen den Ablauf bei der Erstellung der Sicherheitsdokumentation und die Anforderungen an die Bearbeitung der Dokumente.
- Die Teilnehmenden können die erforderlichen Sicherheitsdokumente selbständig innert kurzer Frist erarbeiten

Als Kursvorbereitung dienten bereits bestehende Weisungen und Vorgaben zu Informationssicherheit und Datenschutz sowie eine aktuelle Übersicht über die vorhandenen Netzwerke, Systeme und Anwendungen. Die Arbeiten zur Leitlinie zur Informationssicherheit, zum Rollen- und Berechtigungskonzept sowie zur Planung von Sicherheitsmassnahmen dienten auch dem Informationsaustausch unter den Teilnehmenden. Die Diskussion aktueller Themen aus dem IT-Sicherheitsbereich zum Abschluss des Kurses vermittelte zusätzliche Impulse, beispielsweise zu den Gefahren bei der Verwendung von mobilen Geräten.

Einführung eines Online-Steuerportals

Der Datenschutzbeauftragte hat von 2010 bis 2013 das Projekt zur Einführung eines Online-Steuerportals begleitet, welches natürlichen Personen ermöglicht, die Steuererklärung online auszufüllen und elektronisch einzureichen. Das Projekt wurde letztes Jahr abgeschlossen und in den laufenden Betrieb überführt.

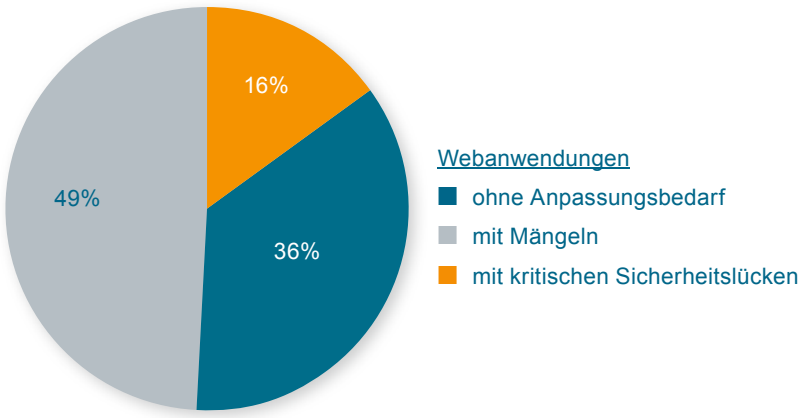
Der Datenschutzbeauftragte war von Beginn an in das Projekt involviert und hat das Steueramt in allen Bereichen der IT-Sicherheit und des Datenschutzes beraten. Die datenschutzrechtlichen Anliegen möglichst frühzeitig einzubringen, ist bei solchen Projekten elementar, um spätere, zeit- und ressourcenaufwendige Korrekturen zu vermeiden.
Zu Beginn des Projekts wurde ein umfassendes Grundlagenpapier zur Sicherheit der Anwendungen erstellt, das die notwendigen Massnahmen für die Entwicklung und den Betrieb von Fachanwendungen festlegte. Die aufgeführten Massnahmen wurden anschliessend im Datenschutz- und Informationssicherheitskonzept des Projekts berücksichtigt.
Eine umfassende Beratung erfolgte in Bezug auf die Frage, ob die konzeptionellen Vorgaben in den Pilotbetrieb eingeflossen waren und ob noch Lücken im organisatorisch-technischen Teil bestanden. Konkret prüfte der Datenschutzbeauftragte die Verträge der Auftragnehmenden, das Sicherheitskonzept, das Betriebshandbuch und die Berechtigungsvergabe. Dazu wurden Interviews mit den Verantwortlichen der Auftragnehmenden und des Steueramts geführt sowie die vorgelegten Dokumente beurteilt. Es wurde festgestellt, dass in allen vier Bereichen (Service Level Agreements, Einbettung Information Security Management System respektive IT-Sicherheitskonzept, Betriebshandbuch sowie Rollen- und Berechtigungskonzept) Ergänzungen notwendig waren. Die Resultate wurden mit der Projektleitung und den Verantwortlichen des Steueramts ausführlich diskutiert und umgesetzt.

Kontrollen unter Einsatz eines Webscanners

Erstmals hat der Datenschutzbeauftragte 2013 im Rahmen seiner Kontrollen einen Webscanner eingesetzt. Schwerpunkt waren die Websites von Schulen. Es konnten zahlreiche kritische Sicherheitslücken aufgedeckt werden.

Regelmässig erscheinen in den Medien Berichte, dass Datenbanken gehackt und die entwendeten Daten publiziert oder für weitere Angriffe, wie beispielsweise Identitätsdiebstahl, missbraucht wurden. Meist liegt die Ursache in der Verwendung unsicherer Webapplikationen. Dies veranlasste den Datenschutzbeauftragten, bei der Kontrolle von Webanwendungen durch Schulen einen Schwerpunkt zu setzen.
Insgesamt kamen über 800 Webanwendungen zur Überprüfung in Frage. Basierend auf einer Risikoanalyse wählte der Datenschutzbeauftragte schliesslich 179 Anwendungen für eine Kontrolle aus. Um die Prüfung möglichst effizient durchzuführen, wurde ein so genannter «Web Application Scanner» eingesetzt. Dieser prüft die Webanwendungen automatisiert und beurteilt die gefundenen Schwachstellen nach ihrer Sicherheitsrelevanz. Die Grafik rechts gibt einen Überblick über die Resultate der Kontrolle. 15% der geprüften Anwendungen wiesen kritische Schwachstellen auf. Dies bedeutet, dass über das Internet auf interne Daten zugegriffen werden konnte. Kurz nach den Kontrollen wurde ein Grossteil der relevanten Sicherheitslücken geschlossen.
Bei den Webanwendungen mit Mängeln kann im Gegensatz zu den Webanwendungen mit kritischen Schwachstellen nicht ohne weiteres via Internet auf interne Daten zugegriffen werden. Dennoch erhöhen auch kleinere Mängel das Risiko und sollten möglichst bald behoben werden. Wegen des hohen Prozentsatzes an kritischen Schwachstellen und der unveränderten Risikolage wird der Datenschutzbeauftragte weiterhin Webanwendungen kontrollieren.

Massnahmen bei Webanwendungen



Kontrolle des Schengener Informationssystems (SIS)

Der Datenschutzbeauftragte hat die Nutzung des Schengener Informationssystems (SIS) durch die Kantonspolizei überprüft.

Das SIS ist ein europäisches Fahndungssystem, in dem Personen ausgeschrieben werden, die polizeilich gesucht, mit einer Einreisesperre versehen oder vermisst werden. Seit dem Beitritt der Schweiz zum Schengener Abkommen im Jahr 2008 haben schweizerische Behörden, unter anderem auch die Kantonspolizei, Zugriff auf diese Fahndungsdatenbank.
Der Inhalt der Kontrolle durch den Datenschutzbeauftragten betraf die Zugriffsverwaltung, die Rechtmässigkeit und Verhältnismässigkeit der implementierten Zugriffsrechte, die organisatorische Umsetzung der Informationssicherheit sowie die rechtmässige Bearbeitung der Informationen in Einzelfällen. Zu diesem Zweck fanden Besprechungen, Interviews, Besichtigungen sowie die Auswertung von Zugriffsprotokollen statt. Das System selbst, das durch das Bundesamt für Polizei betrieben wird, war nicht Teil der Kontrolle.
Mit Ausnahme einer Feststellung gab die Kontrolle keinen Anlass zu Beanstandungen, die sofortiges Handeln erforderlich gemacht hätten. Einzelne Bemerkungen betrafen die Bereiche Benutzerberechtigungen, Outsourcing und Funktionskontrolle des Systems.

Festgestellt wurde aber, dass einzelne Polizeistationen Personen, die sich neu in einer Gemeinde angemeldet hatten, systematisch mit den Einträgen in den Informationssystemen RIPOL und SIS abglichen. Eine solche verdachtsunabhängige Überprüfung aller Neuzuzügerinnen und Neuzuzüger wird von den geltenden Rechtsgrundlagen nicht gedeckt. Rechtmässig ist lediglich die Abfrage im Einzelfall bei Bestehen eines Verdachts. Die Kantonspolizei erliess daraufhin die Weisung, solche systematischen und verdachtsunabhängigen Abfragen zu unterlassen.
Gemäss der Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro sind auch schweizweit koordinierte Kontrollen der Nutzung des SIS vorgesehen. Ein koordinierte Kontrolle hat aber bisher noch nicht stattgefunden.

Kontakt

E-Mail	datenschutz@dsb.zh.ch
Internet	www.datenschutz.ch
Twitter	twitter.com/dsb_zh
Telefon	+41 (0)43 259 39 99
Fax	+41 (0)43 259 51 38
Adresse	Datenschutzbeauftragter des Kantons Zürich, Postfach, CH-8090 Zürich

Impressum

Herausgeber: Datenschutzbeauftragter des Kantons Zürich, Postfach, 8090 Zürich
Korrektorat: Text Control AG, Zürich
Layout: René Habermacher, Visuelle Gestaltung, Zürich
Druck: Kantonale Drucksachen- & Materialzentrale KDMZ, Zürich
Auflage: 800

ISSN 1422-5816

dsb

datenschutzbeauftragter
kanton zürich

www.datenschutz.ch

Datenschutz mit Qualität