dsb

datenschutzbeauftragter
kanton zürich

2014

Tätigkeitsbericht

«Datenschutz schafft Transparenz für die Bürgerinnen und Bürger im Umgang mit ihren Daten.»

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 2014 bis und mit 31. Dezember 2014 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, März 2015

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

Inhaltsverzeichnis

Inhaltsverzeichnis

Vernehmlassungen

Kontrollen und Vorabkontrollen

Datenschutzbeauftragter Kanton Zürich

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

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

- Bei öffentlichen Organen überprüft er mittels Kontrollen (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.

Überblick

«Der korrekte Umgang mit den Personendaten im Unterricht wie in der Schulverwaltung trägt automatisch zum Verständnis eines liberalen Grundrechts unserer Gesellschaft bei.»

In der Schule: D wie Datenschutz

Die neuen Informatikmittel in der Schule sind im Unterricht wie auch in der Verwaltung nicht mehr wegzudenken. Der Umgang mit dem Datenschutz hat Vorbildfunktion.

Schülerinnen und Schüler nutzen den Computer in der Freizeit wie auch für den Unterricht. Der Umgang mit den neuen Kommunikations- und Informatikmitteln ist für die «Digital Natives» so selbstverständlich, dass eher darauf hingewiesen werden muss, dass es neben Smartphone und Internet noch andere Dinge im Leben gibt. Die vielen Angebote im Internet nutzen sie unbeschwert – unbeschwert auch von der Frage, ob ihre persönlichen Informationen sicher sind und wer wohl alles Zugriff auf diese haben könnte. Allerdings nur bis zu einem gewissen Punkt: Der Missbrauch der eigenen Daten oder das digitale Mobbing wird scharf verurteilt, und spätestens bei dieser Problematik beginnen die Jugendlichen sich darüber Gedanken zu machen, was mit ihren Daten geschieht.

Sensibilisierung im Medienunterricht

Der Datenschutzbeauftragte hat auch 2014 mit einigen Schulklassen auf verschiedenen Schulstufen im Rahmen des Medienunterrichts über den Umgang mit den eigenen Daten diskutiert. Dabei stand die Frage im Vordergrund: Warum muss ich meine Daten schützen? Damit wird direkt das Fundament des Datenschutzes angesprochen: die persönliche Freiheit, der Schutz der Privatsphäre und die informationelle Selbstbestimmung. Dass jede und jeder über die eigenen Daten sowie ihre Veröffentlichung und Weitergabe selber bestimmen möchte, ist als Ziel breit akzeptiert und die Verwendung durch andere zu unbestimmten Zwecken – wie dies Allgemeine Geschäftsbedingungen oftmals transparent machen – vielen suspekt. Es gilt daher – beispielsweise im Umfeld der sozialen Netzwerke – sich darüber klar zu werden, welche Daten und Informationen man teilen möchte, da das Risiko des Missbrauchs sehr hoch ist. In den Gesprächen mit Jugendlichen zeigte sich einerseits, dass sie aufgrund zunehmender Aufklärung heute auch bewusster mit ihren eigenen Daten umgehen und den Schutz ihrer Privatsphäre thematisieren.

Verantwortung Schule

Die Schulen können den verantwortungsbewussten Umgang mit den neuen Medien im Unterricht auf allen Stufen berücksichtigen. Ein wichtiger Aspekt ist dabei, dass sie sich selber als Vorbild sehen und neue Informations- und Kommunikationsmittel datenschutzgerecht einsetzen. Dies ist nicht immer einfach, da den Schulen viele Produkte angeboten werden, welche die Voraussetzungen eines datenschutzkonformen Einsatzes nicht erfüllen. Heute sind es zahlreiche Anwendungen im Rahmen des Cloud Computing, die es den Schulen standardmässig nicht erlauben, ihre datenschutzrechtliche Verantwortung wahrzunehmen. Mit der Verwendung von Clouddiensten geht die Kontrolle über die Daten verloren, sie werden irgendwo im Ausland gespeichert und der Zugriff

sowie die Verwendung der Daten durch den Cloudanbieter sind nicht ausgeschlossen.
Der Datenschutzbeauftragte hat im vergangenen Jahr verschiedene dieser Produkte geprüft. Die wenigsten erfüllen die gesetzlichen Anforderungen an Datenschutz und Informationssicherheit. Soweit aber mit den Herstellern eine Anpassung der vertraglichen Bedingungen erreicht werden konnte (Seite 23), lassen sich diese nunmehr auch datenschutzkonform einsetzen. Auf die anderen Produkte ist entweder zu verzichten oder die Verwendung ist auf nicht personenbezogene Daten und Informationen zu beschränken.

Sicherheit in den Schulen

Die Sicherheit der Informationen ist die Grundlage für einen korrekten Umgang mit Personendaten. Der DSB hat deshalb ausgewählte Schulen kontrolliert und dabei festgestellt, dass die technischen Massnahmen überwiegend angemessen implementiert wurden (Seite 34). In zahlreichen Fällen fehlt es aber an klaren organisatorischen Richtlinien, die die Verantwortlichkeiten und Zugriffsberechtigungen regeln.

Weiter hat der Datenschutzbeauftragte die Websites diverser Schulen auf Schwachstellen hin analysiert (Seite 48). Dabei kamen bei allen Websites Sicherheitslücken zum Vorschein, teilweise hätten sogar die Inhalte verändert werden können. Zudem zeigte sich, dass in vielen Websites Programme von Drittanbietern eingebunden waren, die Daten der Benutzerinnen und Benutzer an diese übermitteln. Die Schulen wurden entsprechend informiert. Angesichts der weit verbreiteten Mängel wird der Datenschutzbeauftragte weitere Kontrollen in diesem Bereich vornehmen.

Lexikon für die Schulen

Die Schulen bearbeiten zahlreiche auch sehr sensitive Personendaten. In der Beratungspraxis des Datenschutzbeauftragten beziehen sich viele Anfragen immer wieder auf diesen Themenkomplex. Für den Bereich der Volksschulen hat der Datenschutzbeauftragte deshalb die häufigsten Fragen zum Datenschutz und zur Informationssicherheit zusammengestellt und mit den interessierten Stellen besprochen. Das Resultat ist ein Datenschutzlexikon, das eine Hilfe im Alltag für alle im Schulbereich tätigen Personen darstellt (Seite 24). Es ist auf www.datenschutz.ch erhältlich. Für die übrigen Schulstufen sind ähnliche Hilfsmittel in Planung.
Der Bildungsauftrag der Schulen ist thematisch sehr breit. Der Datenschutz als Querschnittsmaterie spielt dabei nicht nur im Unterricht eine Rolle, sondern berührt die gesamte Institution Schule. Der korrekte Umgang mit den Personendaten im Unterricht wie in der Schulverwaltung trägt dabei automatisch zum Verständnis eines liberalen Grundrechts unserer Gesellschaft bei.

Weitere Schwerpunkte

- Kontrollen auf Anlass
- Einsicht und Berichtigung im Patientendossier
- Datenschutz im Bereich der Spitex
- Einsatz von Videokameras

Kontrollen auf Anlass

Das Gesetz überträgt dem Datenschutzbeauftragten Aufsichts- und Kontrollaufgaben in den Bereichen Datenschutz und Informationssicherheit. Diesen kommt der DSB mit den Datenschutz-Reviews nach, die nach festgelegtem Prüfplan und Methoden der Informatikrevision durchgeführt werden. Bei konkreten Vorfällen nimmt er auch anlassbezogene Kontrollen vor.

Das verfassungsmässige Recht auf Schutz der Privatsphäre beziehungsweise auf Wahrung der informationellen Selbstbestimmung enthält zwei Komponenten: Es führt einerseits zu einer Verpflichtung des Staates, mit geeigneten rechtlichen, organisatorischen und technischen Massnahmen für eine rechtskonforme und verhältnismässige Datenbearbeitung zu sorgen (systemischer Datenschutz). Anderseits bietet es betroffenen Personen Individualrechte, mit denen sie ihren Anspruch auf Wahrung der Privatsphäre gegenüber Datenbearbeitern einfordern und durchsetzen können (individueller Datenschutz).

Der Datenschutzbeauftragte beaufsichtigt die Datenbearbeitungen der öffentlichen Organe. Dazu führt er von sich aus oder auf Anlass Kontrollen durch. Die Kontrolle auf Anlass soll das betroffene öffentliche Organ im Hinblick auf künftige Fälle sensibilisieren und im Bedarfsfall dazu veranlassen, Massnahmen zu treffen.

Kontrollen auf Anlass erfolgen auf beiden Ebenen. Bei der Kontrolle des systemischen Datenschutzes geht es um den Umgang des öffentlichen Organs mit Personendaten. Bestehen Anhaltspunkte für nicht datenschutzkonforme Datenbearbeitungen, prüft der Datenschutzbeauftragte diese näher, insbesondere wenn

- die Datenbearbeitungen eine Vielzahl von Personen betreffen,
- besondere Personendaten bearbeitet werden,
- die Art und Weise von Datenbearbeitungen sensibel ist (beispielsweise durch den Einsatz bestimmter Technologien, komplexe Bearbeitungsabläufe, mehrere beteiligte Stellen mit unterschiedlicher Verantwortung etc.)
  oder
- gesetzliche Grundlagen fehlen beziehungsweise unklar ist, ob diese für die konkrete Datenbearbeitung genügen.

Auf der individualrechtlichen Ebene geht es darum, für den korrekten Umgang des öffentlichen Organs mit den Rechtsansprüchen von einzelnen Gesuchstellenden zu sorgen. Bestehen konkrete Anhaltspunkte, dass ein öffentliches Organ ein Gesuch um Auskunft über eigene Personendaten beziehungsweise auf Berichtigung oder Löschung von Daten nicht korrekt behandelt, interveniert der Datenschutzbeauftragte vorerst im Rahmen seiner Beratungs- und Vermittlungsaufgaben. Sind die Mängel gravierend oder implizieren sie eine möglicherweise fehlerhafte Rechtsanwendung des öffentlichen Organs, klärt der Datenschutzbeauftragte die Situation mittels einer Kontrolle.

Vorgehen bei Kontrollen auf Anlass

Der Datenschutzbeauftragte kann Auskünfte über das Bearbeiten von Personendaten verlangen, Einsicht in Daten nehmen und sich Bearbeitungen vorführen lassen. Die öffentlichen Organe sind zur Mitwirkung verpflichtet, und allfällige Schweigepflichten des öffentlichen Organs stehen der Kontrolle nicht entgegen.

Eine Kontrolle des DSB auf Anlass verläuft nach folgendem standardisierten Ablauf des Datenschutz-Reviews und kann an die jeweilige Fallkonstellation angepasst werden:

1. Entscheid: Der DSB prüft aufgrund von Meldungen und Feststellungen, ob eine Kontrolle angezeigt ist.
2. Ankündigung: Der DSB wendet sich an das öffentliche Organ, schildert Sachverhalt und Anlass der Kontrolle und verlangt eine Stellungnahme (allgemein oder mit einem Fragenkatalog) sowie sachdienliche Unterlagen.
3. Sachverhaltsanalyse: Der DSB wertet die Stellungnahme aus und erstellt den Sachverhalt (möglicherweise mit offenen Punkten). Es erfolgt eine erste rechtliche Beurteilung im Hinblick auf weitere Nachfragen und Abklärungen vor Ort.
4. Kontrolle vor Ort: Der DSB prüft die Datenbearbeitungen vor Ort wie Abläufe, Dossiers, Informatiksysteme etc. und führt Interviews mit Entscheidungsträgern und Mitarbeitenden des öffentlichen Organs.
5. Auswertung: Der DSB wertet die erhaltenen Informationen aus und nimmt rechtliche und technisch-organisatorische Bewertungen vor. Bei Bedarf erfolgen weitere Abklärungen gemäss den Schritten 2 bis 4.
6. Bericht: Der DSB erstellt einen Bericht über seine Feststellungen und Schlussfolgerungen sowie über die zu treffenden Massnahmen. In schwerwiegenden Fällen ordnet er Massnahmen mittels formeller Empfehlung an. Der Bericht beziehungsweise die Empfehlung kann publiziert werden.

§ 35 Abs. 1 und 2 IDG
§ 35 Abs. 1 in Verbindung mit § 38 IDG
§ 36 IDG

Auswertungen von Telefon- und E-Mail-Daten

Im Herbst 2013 wurde bekannt, dass die Universität Zürich der Staatsanwaltschaft verschiedene Daten von Angehörigen der Universität sowie von Dritten herausgegeben hatte und dazu eine unbekannte Menge an Telefon- und E-Mail-Daten auf bestimmte Kontakte hin überprüft worden waren. Das Vorgehen stand im Zusammenhang mit einer Strafanzeige, welche die Universität im September 2012 erstattet hatte. Der Datenschutzbeauftragte leitete bei der Universität eine Kontrolle ein, um die Rechtmässigkeit dieser Datenbearbeitungen zu prüfen.

Die Kontrolle ergab, dass die Universität unrechtmässig Telefon- und E-Mail-Verkehrsdaten ihrer Mitarbeitenden und Studierenden sowie von Mitarbeitenden externer Stellen und assoziierter Institute ausgewertet hatte. Aufgrund der Ergebnisse wurden Daten von Personen, die Verbindungen mit bestimmten Telefonnummern hatten oder E-Mails an bestimmte E-Mail-Adressen oder E-Mail-Domains gesandt hatten, an die Staatsanwaltschaft herausgegeben. Für die Auswertungen, die einer Rasterfahndung entsprachen, verfügt die Universität über keine Rechtsgrundlagen, und die Auswertungen waren auch nicht verhältnismässig. Die Weitergabe der Daten an die Staatsanwaltschaft erfolgte zwar gestützt auf Bestimmungen über die strafprozessuale Rechtshilfe, verletzte jedoch – da die Daten unrechtmässig beschafft worden waren – überwiegende private Interessen der betroffenen Personen und war deshalb ebenfalls unrechtmässig.

Der Datenschutzbeauftragte teilte die Ergebnisse der Kontrolle der Universität mit und forderte sie auf, Massnahmen zu treffen, damit sich solche Ereignisse nicht wiederholen. Er verlangte auch, dass die Betroffenen über die Auswertungen und Datenweitergabe an die Staatsanwaltschaft informiert wurden. Diesen Aufforderungen ist die Universität nachgekommen.

Monitoring einer politischen Gruppierung

In einer Gemeinde war eine neue Gruppierung entstanden, die sich aktiv an der Kommunalpolitik beteiligte. Dies veranlasste die Exekutive, ein (Medien-)Monitoring über diese Gruppierung zu machen. Das Monitoring, von einer externen Kommunikationsagentur durchgeführt, dauerte rund dreieinhalb Monate und führte zu zwei Berichten.

Bei einem Medienmonitoring werden öffentlich zugängliche Quellen hinsichtlich eines bestimmten Sachverhalts oder Themas ausgewertet. Die Auswertung orientiert sich am Thema, zum Beispiel «Bau eines neuen Sportzentrums». Der Zweck der Datenerhebung zielt somit nicht auf bestimmte Personen oder Organisationen, sondern auf einen Sachverhalt oder ein Thema. Auch Medienmonitoring betreffend die eigene Organisation (Behörde oder einzelne Funktionsträger) ist verbreitet. Der vorliegende Fall lag jedoch anders. Bei diesem Monitoring ging es darum, Aktivitäten und Äusserungen einer bestimmten Organisation sowie Haltungen Dritter zu dieser Vereinigung zu beobachten.

Der Datenschutzbeauftragte prüfte dieses Monitoring, nachdem er auf die Vorgänge aufmerksam und von mehreren Personen kontaktiert worden war. Er beurteilte das Vorgehen der Exekutive als unverhältnismässig. Weder der Umstand der Neupositionierung der Kommunikationspolitik durch

die Exekutive noch die Beschränkung des Monitorings auf öffentliche Quellen legitimieren eine systematische Beobachtung einer einzelnen politischen Gruppierung. Als verhältnismässig wäre die Situation zu beurteilen gewesen, wenn sich die Exekutive nach dem Auftreten der neuen Gruppierung in der kommunalpolitischen Landschaft im Sinne einer Momentaufnahme ein Bild darüber verschafft hätte, wer die Gruppierung ist, was sie will und welche Themen für die Exekutive von Interesse sind. Ein Monitoring über einen unbestimmten oder längeren Zeitraum geht jedoch zu weit. Der Datenschutzbeauftragte verlangte von der betreffenden Exekutive die Vernichtung der Monitoring-Berichte.

Ein weiterer Fall, in dem der Datenschutzbeauftragte eine Kontrolle auf Anlass durchführte, betraf das Einsichtsrecht in die Patientendokumentation (Seite 27).

Kontrollen in den Gemeinden

Mit dem Fokus auf kleinere Gemeinden kontrollierte der DSB auch 2014, ob Informationssicherheitsmassnahmen umgesetzt und rechtliche Rahmenbedingungen eingehalten wurden. Erstmals seit der Einführung dieser Reviews wurden Gemeinden aufgrund der Periodizität wiederholt kontrolliert.

Die im Jahr 2013 begonnene Kontrolle von Gemeinden, die weniger als 4000 Einwohnerinnen und Einwohner aufweisen, wurde 2014 fortgesetzt. Die Resultate waren vielversprechend in dem Sinne, dass bei zwei der geprüften Gemeinden keine Massnahmen mit Frist ausgesprochen werden mussten. Dies bedeutet erstens, dass die vom IDG vorgegebenen organisatorischen und technischen Massnahmen so umgesetzt worden waren, dass die Informatiksysteme angemessen geschützt sind. Zweitens heisst es auch, dass die damit bearbeiteten Informationen angemessen geschützt sind, und drittens, dass die rechtlichen Rahmenbedingungen zur Bearbeitung von Personendaten eingehalten wurden. Diese Resultate deuten darauf hin, dass die vom Datenschutzbeauftragten zur Verfügung gestellten, laufend aktualisierten und auf die Grösse der öffentlichen Organe zugeschnittenen Arbeitsdokumente genutzt werden und ihre Wirkung entfalten. So ist es heute möglich, auch in kleinen Gemeinden mit knappen personellen Ressourcen ein angemessenes Sicherheitsniveau zu erreichen.

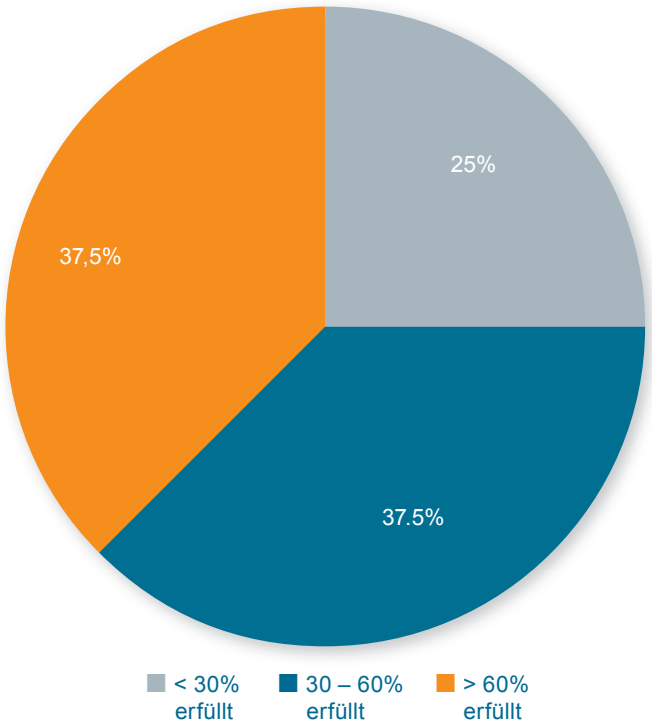
Die von zwei Gemeinden angeforderte Überprüfung der Massnahmen im Bereich der Informationssicherheit fand aufgrund eines Wechsels der Dienstleister statt. Auch hier zeigte sich, dass die Hilfsmittel des Datenschutzbeauftragten eine wertvolle Umsetzungshilfe waren.

Zudem wurden weitere Gemeinden geprüft, bei denen der Datenschutz-Review mehrere Jahre zurücklag. Leider waren hier keine durchgehend zufriedenstellende Resultate zu konstatieren. Der Umsetzungsgrad der gesetzlich geforderten Informationssicherheitsmassnahmen variierte relativ stark von «nicht zufriedenstellend» bis «angemessen». Massnahmen in den Bereichen IT-Strategie, IT-Sicherheitskonzept, Sensibilisierung und Schulung sowie mobile Geräte wurden teilweise nicht oder nicht vollständig umgesetzt, obwohl gerade in diesen Bereichen geeignete Vorlagen und Checklisten vom Datenschutzbeauftragten zur Verfügung gestellt werden.

Der Datenschutzbeauftragte aktualisiert die für die Umsetzung der Informationssicherheit massgebenden Vorlagen und Checklisten laufend. Die aufgrund der Kontrollen evaluierten Bedürfnisse der Gemeinden, die Grösse der Verwaltungseinheiten sowie die neuesten Änderungen der internationalen Standards fliessen jeweils in die Überarbeitung ein. So stehen den Gemeinden auf der

DSB-Website nicht nur revidierte und an die neuesten Anforderungen des Grundschutzkatalogs des deutschen Bundesamts für Sicherheit in der Informationstechnik angepasste Massnahmenkataloge für ihre Planung und Umsetzung der Sicherheitsmassnahmen zur Verfügung – auch beim Einführungsdokument in die Informationssicherheit, das in Form eines Leitfadens vorliegt, wurde Wert auf eine noch effizientere und einfachere Vorgehensweise gelegt.

Erfüllungsgrad der vom IDG geforderten Informationssicherheitsmassnahmen aller geprüften Stellen 2014



Auslagerung – komplex und doch einfach

Öffentliche Organe gehen immer mehr dazu über, ihre Informationen durch externe IT-Dienstleister bearbeiten zu lassen. Die Versuchung, auch die Verantwortung auszulagern, ist gross. Umso wichtiger ist es, sich einen Überblick über die datenschutzrechtlichen Anforderungen zu verschaffen. Der Leitfaden «Bearbeiten im Auftrag», die «AGB Auslagerung Informatikleistungen» und die «AGB Datenbearbeitung durch Dritte» des DSB leisten dabei wertvolle Hilfe.

Das Thema Auslagerung bildete auch 2014 einen Arbeitsschwerpunkt beim Datenschutzbeauftragten. So erkundigte sich beispielsweise eine Schule, ob sie eine bestimmte Software zum Bearbeiten der Schuldaten einsetzen darf. Teilweise waren die zu überprüfenden Produkte bereits im Einsatz. Oder eine Gemeinde reichte Verträge zur Überprüfung der datenschutzrechtlichen Aspekte ein. Vielfach wurde auch eine Beratung gewünscht, welche technischen Massnahmen konkret umgesetzt werden müssen und ob diese Umsetzung praxistauglich ist. Einfach zu implementierende und auf dem Markt angebotene Produkte entsprechen nicht immer den Anforderungen des Datenschutzes. Der Datenschutzbeauftragte schlug jeweils eine datenschutzkonforme alternative Lösung vor.

Mit den Anforderungen vertraut machen

Wer das Bearbeiten von Informationen auszulagern plant, muss sich mit den datenschutzrechtlichen Anforderungen befassen. Dies bedingt eine Auseinandersetzung mit rechtlichen, organisatorischen und technischen Aspekten. Die wichtigste Frage, die es dabei zu klären gibt, ist diejenige, was eine Auslagerung – also eine Bearbeitung durch Dritte – überhaupt ist. Der Gesetzgeber hat nicht explizit definiert, wer unter «Dritten» zu verstehen ist, sondern überlässt diese Auslegung denjenigen, welche die Gesetze anwenden. So können Dritte beispielsweise Amtsstellen anderer Direktionen, andere öffentliche Organe im Kanton, aber auch andere öffentliche Organe ausserhalb des Kantons oder private Anbieter sein. Da Auftragnehmer die Informationen nur in dem Rahmen bearbeiten dürfen, in dem auch das öffentliche Organ dazu berechtigt ist, müssen die Informationen mit angemessenen organisatorischen und technischen Massnahmen geschützt werden. Auch diese Formulierung bedarf in der Praxis der Auslegung. Der Datenschutzbeauftragte orientiert sich jeweils an international geltenden Standards, wie sie vom deutschen Bundesamt für Sicherheit in der Informationstechnik entwickelt wurden.

Sich wandelnde technische Massnahmen

Wird das Bearbeiten sensitiver Informationen ausgelagert, werden diese im Ausland bearbeitet oder werden gar Cloud-Services in Anspruch genommen, sind Massnahmen zum Schutz der Persön-

lichkeitsrechte besonderes wichtig – insbesondere die Verschlüsselung. Dabei geht es um die Verschlüsselung des Transports und der Ablage sowie um das Schlüsselmanagement. Auch neue technische Entwicklungen müssen beobachtet und laufend analysiert werden.

Vertragliche Bestimmungen

Bei Verträgen prüft der Datenschutzbeauftragte unter anderem die Kriterien Kontrolle und Transparenz, den geografischen Ort der Datenbearbeitung, das anwendbare Recht und den Gerichtsstand. Es ist beispielsweise undenkbar, dass ein öffentliches Organ des Kantons Zürich in den USA seine Ansprüche nach amerikanischem Recht geltend machen müsste. Deshalb ist es wichtig, diese Punkte im Vertrag oder in den Allgemeinen Geschäftsbedingungen zu verankern. Solange diese nicht einseitig abänderbar sind, wird dem Schutz der Persönlichkeitsrechte Rechnung getragen.

Leitfaden «Bearbeiten im Auftrag»

Die zahlreichen Anfragen und Beratungen haben den Datenschutzbeauftragten bewogen, einen Leitfaden «Bearbeiten im Auftrag» zu erarbeiten. Darin finden sich nützliche Dokumente, um eine Auslagerung systematisch anzugehen. Es sind dies eine Checkliste zum Vorgehen, ein Überblick über die vertragsrelevanten Bestimmungen inklusive Hinweis, welche Allgemeinen Geschäftsbedingungen oder anderen Bestimmungen in das Vertragswerk einzubinden sind, sowie ein Überblick über die erforderlichen Informationssicherheitsmassnahmen. Die Praxis zeigt, dass jede Software einzeln in Bezug auf diese Anforderungen analysiert werden muss. Dabei bleibt genügend Spielraum, die Nutzung des jeweiligen Produktes im Rahmen des gesetzlichen Ermessens genauer zu bestimmen.

Allgemeine Geschäftsbedingungen

Je nach Art der Auslagerung stehen auf der Website des Datenschutzbeauftragten verschiedene Allgemeine Geschäftsbedingungen zur Verfügung. Diese konkretisieren die wichtigsten gesetzlichen Anforderungen. Werden sie oder analoge Bestimmungen in die Verträge integriert, sind die wichtigsten datenschutzrechtlichen Anforderungen erfüllt. Danach gilt es, den Inhalt umzusetzen und die Umsetzung zu kontrollieren. Werden Informatikleistungen von Dritten in Anspruch genommen, stehen die Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen, kurz «AGB Auslagerung Informatikleistungen», zur Verfügung. Für Vertragsverhältnisse, deren zentraler Bestandteil die Bearbeitung von Informationen für ein öffentliches Organ ist, kann Bezug auf die Allgemeinen datenschutzrechtlichen Geschäftsbedingungen bei der Datenbearbeitung durch Dritte, kurz «AGB Datenbearbeitung durch Dritte», genommen werden. Für alle anderen Fälle stehen Musterformulierungen zu Verfügung.

§ 6 IDG
§ 25 IDV

Konsolidierter Entwicklungs- und Finanzplan 2015–2018

Datenschutzbeauftragter

Nr. 9071
Funktionale Gliederung: 0

Finanzierung

Erfolgsrechnung (in Mio. Fr.)	R 13	B 14	Δ(P 15)	P 15	Δ(P 16)	P 16	Δ(P 17)	P 17	P 18	Δ%(13-18)
Ertrag	0.0	0.1	-0.0	0.0	-0.0	0.0	-0.0	0.0	0.0	
Aufwand	-2.0	-2.4	-0.0	-2.4	-0.0	-2.4	0.0	-2.4	-2.4	20.1
Saldo	-2.0	-2.3	-0.1	-2.3	-0.0	-2.4	-0.0	-2.4	-2.4	
Investitionen (in Mio. Fr.)										Ø (13 -18)
Einnahmen										
Ausgaben										
Nettoinvestitionen										
Personal (Beschäftigungsumfang)	8.0	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 Förderung der Umsetzung angemessener Massnahmen im Bereich der Informationssicherheit	2015
E2 Sicherstellen des Datenschutzes im Umgang mit grossen Datenmengen (eGovernment, Open Government Data, Forschung, Big Data)	2016
E3 Kontrolltätigkeit: Gewährleisten einer regelmässigen und nachhaltigen Kontrolle der Datenbearbeitungen	2017

Indikatoren

Indikatoren	Art	R 13	B 14	P 15	P 16	P 17	P 18
Wirkungen							
W1 Anteil umgesetzter Hinweise bei Datenschutz-Reviews (%) (A3)	min.	48	60	60	60	60	60
W2 Anzahl Besuche auf Webseiten (A4)	min.	190800	80'000	180000	180000	180000	180000
Leistungen							
L1 Anzahl Beratungen von Privatpersonen (A4)	max.	525	500	500	500	500	500
L2 Anzahl Vernehmlassungen und Mitberichte (A2)	P	21	18	18	18	18	18
L3 Anzahl Weiterbildungsangebote für öffentliche Organe (A2)	min.	30	15	20	20	20	20
L4 Anzahl Kontrollen (A3)	min.	31	30	40	40	40	40
Wirtschaftlichkeit							

Leistungsgruppe 9071	Budgetentwurf 2015
Budgetkredit Erfolgsrechnung (in Mio. Fr.)	-2.349
Budgetkredit Investitionsrechnung (in Mio. Fr.)	
Leistungsindikatoren L1, L3 und L4	

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

Rechtmässige Datenbearbeitungen

Der Schwerpunkt der Evaluation des IDG galt im Berichtsjahr dem Prinzip der Gesetzmässigkeit.

Gestützt auf das von der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) erarbeitete Konzept wird jedes Jahr ein spezifischer Schwerpunkt des Informations- und Datenschutzgesetzes (IDG) evaluiert (Tätigkeitsbericht 2012, Seite 12). Damit kommt der Datenschutzbeauftragte den Anforderungen an die Berichterstattung gemäss IDG nach, die auch Aussagen über die Wirkung des Gesetzes beinhaltet.

Rechtmässige Datenbearbeitung

Aufgrund des Legalitätsprinzips beruht alles Verwaltungshandeln auf einer rechtlichen Grundlage. Zudem muss das Handeln der Verwaltung im öffentlichen Interesse liegen und verhältnismässig sein. Dies trifft in gleicher Weise auch auf die Datenbearbeitungen der Verwaltung zu. Das IDG hält deshalb fest, dass öffentliche Organe Personendaten bearbeiten dürfen, soweit dies zur Erfüllung der gesetzlich umschriebenen Aufgabe geeignet und erforderlich ist. Damit ergibt sich grundsätzlich das Recht zur Bearbeitung der Daten der Bürgerinnen und Bürger aus der gesetzlichen Aufgabe des öffentlichen Organs. Der Umfang der Datenbearbeitung ist dabei limitiert auf den Aufgabenzweck und die dafür notwendigen Daten.

Besondere Personendaten

Gewisse Datenbearbeitungen beinhalten indessen einen tieferen Eingriff in die Privatsphäre der betroffenen Personen und bergen deshalb höhere Risiken für die Persönlichkeitsrechte. Zu diesen besonderen Personendaten gehören beispielsweise Gesundheitsdaten, Daten im Bereich der sozialen Hilfe oder Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen. Ein Missbrauch solcher Daten kann ein hohes Potenzial für Diskriminierungen oder andere Nachteile für die betroffenen Personen haben.

Die Bürgerinnen und Bürger brauchen deshalb Transparenz, wenn die Verwaltung solche sensitive Daten über sie bearbeitet. Das IDG verlangt deshalb, dass die Voraussetzungen für das Bearbeiten dieser Daten in einer hinreichend bestimmten Regelung in einem formellen Gesetz festgehalten werden. Mit dieser Bestimmung werden Anforderungen der Bundesverfassung und der Kantonsverfassung umgesetzt. Diese verlangen, dass ein Eingriff in die Grundrechte – wie dies ein Bearbeiten von Personendaten beinhaltet – in einem Gesetz geregelt ist, ein schwerwiegender Eingriff in einem formellen Gesetz.

Kantonale Gesetzgebungen

Die Evaluation untersuchte, wie weit der Gesetzgeber im Kanton Zürich diesen Anforderungen an die Rechtmässigkeit in Bezug auf das Bearbeiten besonderer Personendaten nachgekommen ist und damit die verfassungsmässigen Vorgaben und die berechtigten Erwartungen der Bürgerinnen und Bürger erfüllt hat. Dazu wurden die neueren Gesetzgebungen in verschiedenen Bereichen unter-

sucht. Wie sich zeigte, werden die Anforderungen nicht durchwegs erfüllt. Grundsätzlich ist aber festzustellen, dass der Gesetzgeber bemüht ist, die Voraussetzungen für eine rechtmässige Datenbearbeitung zu schaffen, auch wenn die Bestimmtheit der Normen nicht immer gegeben ist. Soweit es sich um schwere Eingriffe in die persönliche Freiheit handelt, kann hier auch korrigierend eingewirkt werden, wie dies das Bundesgericht im Falle des Polizeigesetzes tat (BGE 136 I 87 E. 8.3).

Die Ergebnisse der Evaluation der Gesetzmässigkeit werden wie die letztjährigen Erkenntnisse aus der Bevölkerungsbefragung (Tätigkeitsbericht 2013, Seite 14) in den Schlussbericht einfliessen.

§ 8 IDG
Art. 36 BV
Art. 10 Abs. 2 KV

«Das Recht auf Einsicht in die eigenen Daten ist ein Kernelement des Datenschutzes, von dem Patientinnen und Patienten immer wieder Gebrauch machen.»

Breites Spektrum der Beratungen

Der Einsatz neuer Technologien in der Verwaltung nimmt stetig zu und so mehren sich beim Datenschutzbeauftragten die Anfragen, wie Produkte datenschutzkonform eingesetzt werden können. Im Fokus standen 2014 wiederum die Themen Auslagerung in die Cloud und Einsatz von Videokameras. Dazu kamen zahlreiche Beratungen zur Umsetzung des Kindes- und Erwachsenenschutzrechts, zu den Abrechnungsmodalitäten im Gesundheitsbereich und zum Zugang zu den eigenen Daten.

Neue technische Produkte versprechen ein einfaches und effizientes Bearbeiten von Daten. Von diesen Vorteilen wollen auch die kantonale Verwaltung, die Gemeinden und alle anderen öffentlichen Organe profitieren. Im Rahmen von Anfragen hat der Datenschutzbeauftragte einige dieser Produkte wie Google Classroom, Microsoft Office 365 oder Zscaler mit Blick auf die datenschutzrechtlichen Anforderungen überprüft. Dabei ging es immer auch um Fragen rund um die Auslagerung. Zentral ist, dass das öffentliche Organ die Kontrolle über das Bearbeiten seiner Daten behält. Dabei helfen insbesondere sorgfältige Abklärungen im Vorfeld eines solchen Einsatzes, detaillierte Verträge mit besonderen Schutzmassnahmen für sensible Daten, Transparenz in Bezug auf die Orte der Datenbearbeitung, die Anwendung schweizerischen Rechts und ein Schweizer Gerichtsstand.

Videoüberwachung ist nicht gleich Videoüberwachung. So gehen die neuesten Tendenzen beim Einsatz von Videokameras dahin, diese zur Unterstützung administrativer Tätigkeiten einzusetzen. Unverändert bleibt die Tatsache, dass die dadurch bearbeiteten Daten denselben datenschutzrechtlichen Voraussetzungen unterliegen wie beim Einsatz von Kameras zu den bisher verfolgten präventiven Zwecken. Das heisst, solche Kameras dürfen nur zur Anwendung kommen, wenn keine anderen, weniger in die Persönlichkeitsrechte eingreifenden Mittel zur Verfügung stehen und die Rahmenbedingungen in einem Reglement konkretisiert sind.

Die Umsetzung des Kindes- und Erwachsenenschutzrechts sowie der Zugang zu den eigenen Daten generierten auch 2014 zahlreiche Anfragen an den Datenschutzbeauftragten. Beim Kindes- und Erwachsenenschutzrecht stand die Auslegung der Gesetze in Bezug auf den Informationsaustausch zwischen den Behörden im Zentrum.

Was den Zugang zu den eigenen Daten betrifft, liessen sich Betroffene häufig beraten, wenn es sich um das Bearbeiten ihrer Daten in sensiblen Bereichen wie dem Polizei- und Gesundheitsrecht handelte.

Mit der neuen Spitalfinanzierung änderten sich auch die Regelungen betreffend die Kostenbeteiligung der Kantone. Dies erforderte die Klärung vieler datenschutzrechtlicher Fragen, insbesondere wer welche Daten erhalten darf und wie diese bearbeitet werden.

01
Digitale Datenbearbeitung im Schulzimmer

Die digitale Datenbearbeitung gehört heute in den Schulen zum Alltag. Nicht immer sind die verwendeten IT-Produkte datenschutzkonform. 2014 hat der Datenschutzbeauftragte verschiedene Produkte, insbesondere Google Classroom, Microsoft Office 365 sowie ein Datenbankhosting von LehrerOffice in Bezug auf die datenschutzrechtlichen Anforderungen überprüft.
Diesen Produkten gemeinsam ist, dass es sich bei deren Inanspruchnahme um ein Bearbeiten im Auftrag, also um Informatikleistungen Dritter handelt, da die Daten nicht in der Schule bleiben. Zentral bei einer Auslagerung sind Transparenz und Kontrolle. Es ist zu prüfen, ob der Auslagerung rechtliche Bestimmungen wie Geheimhaltungspflichten entgegenstehen, wie dies beispielsweise bei schulpsychologischen Informationen der Fall ist. Weiter kann die Sensitivität der Daten einer Bearbeitung durch Dritte entgegenstehen. Im Vertrag sind insbesondere Verantwortung, Verfügungsmacht, Zweckbindung, Geheimhaltungsverpflichtungen, Rechte der Betroffenen, Informationssicherheitsmassnahmen, Kontrollmöglichkeiten, Unterauftragsverhältnisse, Ort der Datenbearbeitung, anwendbares Recht und Gerichtsstand zu regeln. Beinhaltet die Auslagerung die Inanspruchnahme eines Cloud-Services, müssen die eingesetzte Technologie und sämtliche Datenbearbeitungsorte zudem dokumentiert werden. Weiter dürfen Informationsbestände mit besonderen Personendaten nur mit umfassenden kryptografischen Massnahmen in die Cloud einfliessen. Beinhalten Cloud-Services Datenbearbeitungen im Ausland, muss abgeklärt werden, ob ein der Schweiz gleichwertiges Datenschutzniveau besteht und/oder zusätzliche Sicherheitsmassnahmen umgesetzt werden müssen.
Eine Schule konsultierte den Datenschutzbeauftragten im Hinblick auf die beabsichtigte Nutzung von Google Classroom – einem Produkt, das Lehrpersonen im Rahmen von «Apps for Education» den Unterricht und die Kommunikation innerhalb der Klasse erleichtert. Die Prüfung der Nutzungsbestimmungen ergab, dass unter anderem Daten weltweit bearbeitet werden, der Gerichtsstand sich in den USA befindet und amerikanisches Recht anwendbar ist. Weiter war intransparent, welche Daten Google an wen zu welchem Zweck weitergibt. Aus diesen Gründen genügt Google Classroom den datenschutzrechtlichen Anforderungen nicht.
Eine Schulgemeinde legte dem Datenschutzbeauftragten einen Vertrag für ein Datenbank-Hosting von LehrerOffice zur Prüfung vor. Der Vertrag musste mit einigen datenschutzrechtlichen Punkten ergänzt werden. Beispielsweise darf ein Wechsel des Hostingpartners nur mit ausdrücklicher schriftlicher Zustimmung des öffentlichen Organs erfolgen. Datenverluste als Kernelement der Informationssicherheit sollten nicht von der Haftung ausgenommen werden. Weiter musste im Vertrag festgehalten werden, dass im Fall der Vertragsauflösung sämtliche Informationsbestände unentgeltlich an die Schulgemeinde zurückgegeben werden. Geheimhaltungspflichten müssen auch nach Auflösung des Vertrages eingehalten werden. Der Vertrag sollte zudem eine Bestimmung zur Zweckbindung enthalten.
Die vom Auftragnehmer bearbeiteten Informationen dürfen ausschliesslich zum vertraglich festgelegten Zweck verwendet werden. Weitere Verwendungszwecke müssen vom öffentlichen Organ schriftlich bewilligt werden.
Ein Passus betreffend Informationszugangsgesuche musste ebenfalls in den Vertrag aufgenommen werden. Dabei geht es um die Pflicht, allfällig beim Auftragnehmer eingereichte Informationszugangsgesuche an das öffentliche Organ weiterzuleiten und die Beantwortung eines solchen Gesuches zu ermöglichen.

Mehrere Schulen gelangten an den Datenschutzbeauftragten, weil sie Microsoft Office 365, ein Cloud Service, einsetzen wollten. Bei der Prüfung eines solchen Produkts sind die einzelnen Kriterien differenziert zu gewichten. Transparenz, Verfügungsmacht, Bearbeitungsorte, Kontrollrechte, anwendbares Recht und Gerichtsstand sind dabei besonders wichtig. Zudem muss schweizerisches Recht zur Anwendung kommen und der Gerichtsstand muss in der Schweiz liegen. Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, konnte mit Microsoft die vertraglichen Bedingungen so anpassen, dass der Einsatz von Office 365 im Schulbereich möglich ist. Dafür wurde eine speziell für den schweizerischen Bildungsbereich geltende Vertragsergänzung ausgearbeitet, die sicherstellt, dass eine datenschutzkonforme Nutzung gewährleistet ist. Insbesondere sind die Verantwortlichkeiten klar geregelt, die Datenbearbeitungsorte auf Europa beschränkt, die Kontrollmöglichkeiten vorbehalten, schweizerisches Recht anwendbar und der Gerichtsstand liegt in der Schweiz.

§ 6 IDG
§ 7 IDG
§ 25 IDV

02
Datenschutzlexikon und Analyse IT-Sicherheit in den Volksschulen

Der Datenschutzbeauftragte hat die von den Volksschulen am häufigsten gestellten Fragen zu den Themen Datenschutz und Informationssicherheit in einem Datenschutzlexikon beantwortet. Das Lexikon richtet sich an Lehrpersonen, Schulleitungen, Schulverwaltungen, Schulbehörden, Fachpersonen und Eltern und gibt einen Überblick über datenschutzrelevante Anliegen im Schulbereich.
Das Datenschutzlexikon ist Bestandteil eines Projekts, dessen Ziel es ist, die Volksschulen im Kanton Zürich flächendeckend in Bezug auf Datenschutz und Informationssicherheit zu sensibilisieren.
Zudem soll mit einer Umfrage das Niveau der Informationssicherheit erhoben werden. Die Informationen zur Informatikumgebung werden mittels Fragebogen erhoben, in welchem die Schulen die Umsetzung ihrer Informationssicherheitsmassnahmen zum Schutz der von ihnen bearbeiten Daten selbst einschätzen. Der Fragebogen enthält die wichtigsten schulspezifischen Kennzahlen wie Grösse der Schule, installierte Geräte, Anwendungen und personelle Ressourcen im IT-Bereich. Weiter gibt er Auskunft über die implementierten organisatorischen und technischen Massnahmen sowie die IT-Umgebung.
Aufgrund eines Pilotprojekts, für das acht Schulen ausgewählt und angeschrieben wurden, liegen erste Ergebnisse vor. Die Auswertung hat ergeben, dass die technischen Massnahmen mehrheitlich angemessen implementiert wurden. In Bezug auf das Umsetzen der organisatorischen Massnahmen wie Benutzerweisungen oder Rollen- und Berechtigungskonzepte besteht jedoch Handlungsbedarf.
Alle im Rahmen dieses Projekts angeschriebenen Schulen erhalten vom Datenschutzbeauftragten eine Gesamtübersicht über den Stand der Informationssicherheit, eine Beurteilung des Sicherheitsniveaus sowie detaillierte Informationen zum Beheben allfälliger Schwachstellen in ihrem Umfeld.

§ 7 IDG
§ 34 lit. a und c IDG

03
Einsatz der Zscaler Security Cloud

Der Datenschutzbeauftragte wird häufig gebeten zu prüfen, ob Softwareprodukte datenschutzkonform sind – so auch beim Einsatz des Produktes Zscaler Security Cloud durch eine Hochschule.
Zscaler Security Cloud ist ein Produkt, das den Internetverkehr auf Malware überprüft und den Zugriff auf illegale Webseiten sperrt. Bei der Nutzung dieses Produkts wird der Internetverkehr über die Server der Firma Zscaler geleitet, wobei unbekannt ist, an welchen Standorten die Daten bearbeitet werden. Mit Secure Socket Layer (SSL) geschützte Verbindungen, die besondere Personendaten und Passwörter beinhalten, werden durch Zscaler entschlüsselt und überprüft. Werden IT-Dienstleistungen ausgelagert, muss gewährleistet sein, dass die Daten nur zu den definierten Zwecken verwendet, angemessen geschützt und in vorgängig definierten Fristen gelöscht werden. Demzufolge ist ein schriftlicher Vertrag mit Zscaler abzuschliessen. Da der Abschluss eines solchen Vertrages nicht möglich war, konnte die Hochschule Zscaler Security Cloud nicht verwenden.
Der Datenschutzbeauftragte schlug der Hochschule den Einsatz einer datenschutzfreundlicheren Lösung vor, um sich vor den Risiken im Internet zu schützen. Konkret wurden lokal installierte Hardwarelösungen für die Überprüfung des Internetverkehrs vorgeschlagen. Die Firmen Barracuda, Bluecoat, Dell, FortiGate und Palo Alto Networks beispielsweise bieten datenschutzkonforme Lösungen an.

§ 6 IDG
§ 25 IDV
§ 7 IDG

04
Meldungen an das Strassenverkehrsamt

Eine Privatperson reichte dem Strassenverkehrsamt ein Dokument mit Informationen über eine andere Person ein. Das Strassenverkehrsamt eröffnete daraufhin ein Verfahren zur Abklärung der Fahreignung der betroffenen Person. Letztere hatte der das Dokument einreichenden Person ausdrücklich untersagt, das Dokument weiter zu verwenden. Die betroffene Person wandte sich deshalb an den Datenschutzbeauftragten zwecks Klärung der Frage, ob das Strassenverkehrsamt verpflichtet sei, Meldungen auf ihre Rechtmässigkeit zu überprüfen mit der Konsequenz, dass bei einer widerrechtlich erfolgten Meldung kein Verfahren eröffnet werden dürfe.
Der Fahrausweis ist eine sogenannte Polizeierlaubnis, auf die ein Anspruch besteht, sofern die gesetzlichen Voraussetzungen erfüllt sind. Dazu zählt die Fahreignung einer Person. Bestehen Zweifel daran, ist die Person einer Fahreignungsuntersuchung zu unterziehen. Wird dabei festgestellt, dass die körperliche oder geistige Leistungsfähigkeit nicht oder nicht mehr ausreicht, um ein Motorfahrzeug sicher zu führen, wird der Fahrausweis auf unbestimmte Zeit entzogen. Erhält das Strassenverkehrsamt einen Hinweis (zum Beispiel von Polizei, Ärzten oder Privatpersonen), wonach bei einer Person ein Grund zum Entzug des Fahrausweises bestehen könnte, ist es von Am-

tes wegen verpflichtet, ein Verfahren zu eröffnen und den Sachverhalt abzuklären. Zweifel an der Fahreignung können bereits aufgrund weniger Anhaltspunkte bestehen. Die Abklärungen, welche das Strassenverkehrsamt vornimmt beziehungsweise bei einem Arzt in Auftrag gibt, dienen der Erhärtung oder Widerlegung jenes Hinweises. Wie aufschlussreich ein Hinweis sein muss, damit das Strassenverkehrsamt ein Verfahren eröffnet, liegt in dessen Ermessen.

Der Datenschutzbeauftragte kam zum Schluss, dass das Strassenverkehrsamt verpflichtet ist, ein Verfahren zu eröffnen, wenn es aufgrund eines Hinweises zur Ansicht gelangt, dass Zweifel an der Fahreignung einer Person bestehen. Eine Pflicht zur Prüfung, ob eine Meldung rechtmässig erfolgt ist, besteht dabei nicht. Die Verantwortung für die Rechtmässigkeit der Meldung liegt vielmehr bei der meldenden Person, die den Vorschriften des Bundesgesetzes über den Datenschutz unterliegt. Die Feststellung der Widerrechtlichkeit einer Meldung ist deshalb Aufgabe des zuständigen Gerichts bei einer entsprechenden Klage.

Art. 14 Abs. 2, 15d und 16d SVG

05
Berichtigung und Gegendarstellung im Patientendossier

Eine Privatperson wandte sich mit der Frage an den Datenschutzbeauftragten, ob und wie sie ihr Patientendossier bei einer Klinik berichtigen lassen kann. Sie wollte ihre Sicht im Sinne einer Gegendarstellung schildern, um ihre abweichende Wahrnehmung bezüglich des Ablaufs der Geschehnisse aufzuzeigen. Die Klinik schlug ihr vor, dass sie die «Gegendarstellung» dem Patientendossier beifügt und den Austrittsbericht mit folgender Textpassage ergänzt: «Die Patientin stellte am (Datum) ein Gesuch um Berichtigung und Gegendarstellung bei der Klinikleitung. Der Vollständigkeit der Akten halber wird die Gegendarstellung der Patientin dem Austrittsbericht beigelegt. Es sei seitens der Klinik vermerkt, dass keine Zustimmung zu den Gegendarstellungen besteht und die Klinik die Rechtmässigkeit und die fachlich korrekte Durchführung der Behandlung nicht anzweifelt.»
Betroffene Personen können eine Berichtigung verlangen, wenn Personendaten unrichtig sind. Gemäss dem Patientinnen- und Patientengesetz erfolgt im Bereich der Patientendokumentation eine Berichtigung in Form einer Ergänzung. Dabei wird die Patientendokumentation um die Darlegung des Betroffenen, beispielsweise wie sich ein Sachverhalt ereignet hat, ergänzt.
Die von der Klinik vorgeschlagene Ergänzung des Austrittsberichts hält einerseits fest, wie die dem Patientendossier beigelegte «Gegendarstellung» zu qualifizieren ist. Andererseits stellt die Klinik in der Textpassage klar, für welche Inhalte des Patientendossiers sie die Verantwortung übernimmt und für welche nicht. Der Datenschutzbeauftragte kam zum Schluss, dass dieses Vorgehen eine zulässige Verwirklichung des Berichtigungsrechts der betroffenen Person darstellt.

§ 21 lit. a IDG
§ 17 Abs. 3 Patientinnen- und Patientengesetz

06
Recht auf Einsicht in die Patientendokumentation

2014 wandten sich zahlreiche Personen mit Fragen zur Geltendmachung ihres Rechts auf Auskunft im Spital an den Datenschutzbeauftragten.
Patientinnen und Patienten haben das Recht auf Einsicht in ihre Patientendokumentation, in der sämtliche Behandlungen festgehalten werden. Dazu zählen insbesondere Untersuchungen, Diagnosen, Therapie und Pflege. Sie muss auch Auskunft über erfolgte Aufklärungen geben.
Hat die Patientin oder der Patient beispielsweise eine Bezugsperson bezeichnet oder eine Patientenverfügung erstellt, sollte dies ebenfalls in der Dokumentation festgehalten werden.
Die Einsicht kann mit Rücksicht auf schutzwürdige Interessen Dritter eingeschränkt werden. In diesem Fall hat das Spital zu begründen, weshalb es die Einsicht beschränkt. Die Gewährung der Auskunft erfolgt in der Regel schriftlich mittels Zustellung von Kopien beziehungsweise – bei elektronisch geführten Patientendokumentationen – von Ausdrucken.
Das Auskunftsrecht umfasst auch den Anspruch auf Einsicht in die Logdaten (Tätigkeitsbericht 2013, Seite 23). So hatte ein Spital einer Patientin auf Gesuch hin die Logprotokolle zugesandt. Aus diesen war ersichtlich, wer wann auf die elektronische Patientendokumentation der Patientin zugegriffen hatte. Die Patientin machte geltend, dass zahlreiche Personen Zugriff genommen hätten, welche an ihrer Behandlung nicht beteiligt gewesen seien.
Das Spital unterzog die einzelnen Zugriffe einer Prüfung und kam zum Schluss, dass sämtliche Zugriffe in Ausübung der dienstlichen Tätigkeit getätigt worden waren. Es bot der Patientin an, ihr vor Ort die Technik des Klinikinformationssystems zu erläutern. Die Patientin wandte sich daraufhin an den Datenschutzbeauftragten und bat um eine rechtliche Überprüfung des Sachverhalts. Aufgrund der eingereichten Unterlagen bestanden für den Datenschutzbeauftragten keine Anhaltspunkte, dass die Zugriffe unrechtmässig erfolgt waren. Auf entsprechende Nachfrage hin bestätigte das Spital, sämtliche von der Patientin beanstandeten Zugriffe überprüft zu haben. Der Datenschutzbeauftragte empfahl der Patientin deshalb, auf das Gesprächsangebot des Spitals einzugehen.
In einem anderen Fall führte der Datenschutzbeauftragte eine Kontrolle betreffend die korrekte Handhabung des Auskunftsrechts durch. Aufgrund von Unterlagen, welche die Betroffenen vom Spital sowie von Dritten erhalten hatten, bestanden konkrete Anhaltspunkte, dass keine vollständige Auskunft erteilt worden war. Die Kontrolle ergab, dass ein Dokument, in dessen Besitz das Spital hätte sein müssen, nicht vorhanden war. Der Grund für das Fehlen des betreffenden Aktenstücks blieb offen. Im Übrigen gab das Spital an, dass es vollständige Einsicht gewährt habe. Zudem legte es nachvollziehbar dar, wie es für die Gewährung der Einsicht vorgegangen war. Gestützt darauf kam der Datenschutzbeauftragte zum Schluss, dass die Auskunftserteilung gesetzeskonform erfolgt war.
Zum Einsichtsrecht in das Patientendossier und zu weiteren Fragen rund um Patientendaten hat der Datenschutzbeauftragte eine Broschüre herausgegeben, die im Berichtsjahr neu aufgelegt wurde. Die Broschüre findet regen Zuspruch. Sie wird von mehreren Spitälern periodisch in grosser Anzahl bestellt und allen Patientinnen und Patienten abgegeben.

§ 19 Patientinnen- und Patientengesetz
§ 13 Gesundheitsgesetz
§ 20 Abs. 2 IDG in Verbindung mit §§ 16 ff. IDV

07
Empfehlungen zum Datenschutz für die Spitex

Der Spitex Verband Kanton Zürich wollte seinen Mitgliedsorganisationen Unterstützung im Bereich des Datenschutzes bieten und Empfehlungen zum Umgang mit Personendaten erlassen. Er bat deshalb den Datenschutzbeauftragten, die für die Spitex-Organisationen im Kanton Bern bestehenden Datenschutzrichtlinien auf ihre Vereinbarkeit mit den gesetzlichen Bestimmungen im Kanton Zürich zu prüfen, um sie als Grundlage für die zu erarbeitenden Empfehlungen nutzen zu können.
Der Datenschutzbeauftragte und der Spitex Verband erarbeiteten daraufhin in Zusammenarbeit mit der Datenschutzstelle der Stadt Zürich einen Entwurf. Dabei waren verschiedene fachliche und rechtliche Fragen zu klären. Der Spitex Verband unterbreitete den Entwurf anschliessend der Gesundheitsdirektion zur Stellungnahme. Aufgrund der Rückmeldung der Gesundheitsdirektion wurden nochmals einige Anpassungen vorgenommen. Im Herbst 2014 lagen die definitiven Empfehlungen vor, welche der Spitex Verband zuhanden seiner Mitglieder verabschiedete. Die Empfehlungen richten sich an die öffentlich-rechtlich organisierten Spitex-Organisationen sowie an die privatrechtlich organisierten Spitex-Organisationen mit öffentlichem Leistungsauftrag und umfassen folgende Themen:

- Übersicht über rechtliche Grundlagen
- Grundsätze der Bearbeitung von Klientendaten
- Rechte der Klientinnen und Klienten in datenschutzrechtlicher Hinsicht
- Führung, Aufbewahrung und Verwaltung der Klientendokumentation
- Schweigepflichten und deren Durchbrechung bei Datenbekanntgaben an Dritte
- Grundsätze der Informationssicherheit

Mit den Empfehlungen des kantonalen Spitex Verbandes steht den Spitex-Organisationen eine gute Arbeitshilfe für die Lösung datenschutzrechtlicher Fragen zur Verfügung.

08
Rechnungskontrolle bei stationär erbrachten Leistungen

Mit der Einführung der neuen Spitalfinanzierung änderten sich auch die Regelungen zur Kostenbeteiligung der Kantone an den stationären Spitalbehandlungen. Diese sind nach dem Krankenversicherungsgesetz verpflichtet, sich an den Kosten stationärer Spitalbehandlungen zu beteiligen. In diesem Zusammenhang stellten sich verschiedene datenschutzrechtliche Fragen, beispielsweise wie die Rechnungstellung von den Spitälern an die Kantone erfolgt, welche Daten die Rechnungen enthalten und wie die Rechnungskontrolle durchgeführt wird. Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, führte deshalb eine Befragung bei den kantonalen Gesundheitsbehörden durch. Ziel war es, einen Überblick über die Modalitäten des Datenaustauschs zu erhalten.
Der Datenschutzbeauftragte erörterte die Thematik auch mit Vertretern der Gesundheitsdirektion. Dabei zeigte sich, dass der Kanton Zürich eine Rechnungskontrolle durchführt, die im Wesentlichen aus einer Überprüfung des Wohnsitzes zur Klärung der Leistungspflicht sowie einer Plausibilitätsprüfung bezüg-

lich des Rechnungsbetrags besteht. Eine Wirtschaftlichkeitsprüfung findet nicht statt. Aus Sicht des Datenschutzbeauftragten bestand aufgrund der erhaltenen Auskünfte kein unmittelbarer Handlungsbedarf. Die Umfrage in den anderen Kantonen ergab hingegen, dass in vielen Fällen Verbesserungsbedarf beim Umgang mit Rechnungskorrekturen besteht. Oft erfahren die Kantone nicht, wenn eine Krankenversicherung aufgrund ihrer Rechnungs- und Wirtschaftlichkeitsprüfung eine Rechnung korrigiert beziehungsweise den Leistungserbringer zur Neufakturierung auffordert. Dies kann dazu führen, dass diese Kantone zu viel bezahlen. Privatim weist deshalb darauf hin, dass die Kantone die Leistungserbringer in den Leistungsvereinbarungen zur Mitteilung von Rechnungskorrekturen verpflichten können, wie dies in einigen Kantonen – unter anderem im Kanton Zürich – bereits der Fall ist. Alternativ könnte auch im Rahmen einer Revision des Tarifstrukturvertrags SwissDRG eine Mitteilungspflicht der Krankenversicherer an die Kantone eingeführt werden.

Art. 49a KVG

09
Keine anonymisierte Abrechnung von Spitex-Leistungen

Eine Privatperson wandte sich mit der Frage an den Datenschutzbeauftragten, ob die Bekanntgabe des Namens von Personen, die psychiatrische Spitex-Leistungen beziehen, an die Wohngemeinde im Zusammenhang mit der Abrechnung der Leistungen erforderlich ist. Sie regte an, dass Spitex-Organisationen den Gemeinden die Abrechnungen von psychiatrischen Spitex-Leistungen in anonymisierter Form zustellen. Aus Angst vor stigmatisierenden Folgen einer psychischen Erkrankung hatte eine betroffene Person den Kostenanteil der Gemeinde bis anhin selber übernommen. Nach einer Tariferhöhung war sie dazu aber nicht mehr in der Lage.
Nach den Vorschriften des Pflegegesetzes sind die Gemeinden verpflichtet, sich an den Pflegekosten ihrer Einwohnerinnen und Einwohner zu beteiligen, mithin auch an psychiatrischen Spitex-Leistungen. Die Gemeinden entrichten keinen Globalbeitrag, sondern sind zur anteilsmässigen Kostenübernahme nach Massgabe der erbrachten Pflegeleistungen im Einzelfall verpflichtet. Zur Prüfung ihrer Leistungspflicht sind die Gemeinden berechtigt, eine Rechnungskontrolle vorzunehmen. Diese beinhaltet unter anderem die Überprüfung, ob die betroffene Person in der Gemeinde ihren Wohnsitz hat, was die Bekanntgabe des Namens der Leistungsbezügerin beziehungsweise des Leistungsbezügers bedingt. Die Gemeinde kann die Administration und Zahlungsabwicklung der Sozialversicherungsanstalt oder einer anderen geeigneten Stelle übertragen.
Ein Anspruch der betroffenen Person, dass ihr Name bei dieser Stelle verbleibt, ist gesetzlich nicht vorgesehen und würde auch dem Auftragsverhältnis, welches zwischen der Gemeinde und dem beauftragten Dritten besteht, zuwiderlaufen. Der Datenschutzbeauftragte kam daher zum Schluss, dass die Bekanntgabe des Namens zu Abrechnungszwecken rechtmässig ist.

§ 8 Abs. 2 IDG
§§ 9 ff. und 20 f. Pflegegesetz

10
Aufbewahrungsfrist von Unterlagen im Bewerbungsverfahren

Eine Privatperson wandte sich an den Datenschutzbeauftragten, weil sie auf eine Bewerbung bei der Kantonspolizei eine Absage erhalten hatte, die mit Übertretungen begründet wurde, welche mehr als zehn Jahre zurücklagen. Die betroffene Person ging davon aus, dass diese Angaben bereits hätten gelöscht werden müssen. Sie fragte beim Datenschutzbeauftragten nach, ob mehr als zehn Jahre zurückliegende Ereignisse im Rahmen eines Bewerbungsverfahrens beigezogen werden dürfen. Die Person hatte sich mehrfach bei der Kantonspolizei beworben und jeweils ihre Einwilligung gegeben, dass Auskünfte über sie eingeholt werden dürfen. Aus den in früheren Bewerbungsverfahren erlangten Angaben erstellte die Kantonspolizei interne Informationsberichte. Darin waren auch Angaben über Übertretungen enthalten, die über zehn Jahre zurücklagen.

Die betroffene Privatperson stellte auf Empfehlung des Datenschutzbeauftragten zunächst ein Auskunftsgesuch über gespeicherte und neu erhobene Daten bei der Kantonspolizei und erfragte die Quellen der Daten sowie die rechtlichen Grundlagen für die Datenbearbeitung. Die Kantonspolizei erteilte ihr darauf entsprechend Auskunft. Der Datenschutzbeauftragte wandte sich in der Folge an die Kantonspolizei und erkundigte sich über Aufbewahrungsfristen, gesetzliche Grundlagen und den Inhalt des Informationsberichts sowie die Begründung für den Beizug der Angaben zu Übertretungen aus den Jahren 2001/2002. Die Kantonspolizei entgegnete, dass die Absage nicht wegen der Übertretungen, sondern aufgrund des Quervergleichs mit den anderen Bewerbern erfolgt war. Gestützt auf die Einwilligung des Bewerbers würden Auskünfte eingeholt und ein Informationsbericht erstellt, für welchen eine fünfjährige Aufbewahrungsfrist gelte; andere Bewerbungsunterlagen würden lediglich zwei Jahre aufbewahrt. Da die Übertretungen Eingang in den Informationsbericht gefunden hatten und dieser während der Aufbewahrungsfrist bei erneuten Bewerbungen beigezogen wird, konnte die Situation entstehen, dass sich darin Informationen fanden, die älter als zehn Jahre waren.

Der Datenschutzbeauftragte kam zum Schluss, dass das Vorgehen der Kantonspolizei zulässig war, weil die Rechtsgrundlage für den Informationsbericht und seine Aufbewahrungsdauer eine andere ist als für die übrigen Bewerbungsunterlagen. Da Informationen über die mehr als zehn Jahre zurückliegenden Übertretungen Eingang in den Informationsbericht gefunden hatten, wurden sie aufgrund anderer Rechtsgrundlagen und für einen anderen Bearbeitungszweck über die ursprünglich vorgesehene Aufbewahrungsfrist hinaus aufbewahrt.

§ 5 Abs. 2 IDG
§ 34 Abs. 3 PG
§ § 43 und 52 PolG
§ 18 POLIS-Verordnung

11
Meldepflichtverletzung bei Ergänzungsleistungen

Eine Gemeinde wandte sich mit der Frage an den Datenschutzbeauftragten, wie sie beim Steueramt Informationen über eine Ergänzungsleistungen beziehende Person zur Neubeurteilung des Anspruchs erhalten könne. Die Leiterin Soziales habe in ihrer Funktion als Gemeinderätin im Rahmen eines Gesuchs um Steuererlass von relevanten Tatsachen erfahren, die auf eine Meldepflichtverletzung hindeuteten. Gestützt darauf müsste eine Leistungsanpassung geprüft werden. Die Gemeinde wollte wissen, ob sie die Information für eine Rückforderung nutzen könne.

Eine Ergänzungsleistungen beziehende Person ist verpflichtet, wesentliche Änderungen bei den für eine Leistung massgebenden Verhältnissen zu melden. Eine gesetzliche Grundlage für einen Datenaustausch zwischen dem Steueramt und dem Sozialamt liegt nicht vor. Weil zwei unterschiedliche Ämter involviert sind, werden die Personendaten zu unterschiedlichen Zwecken bearbeitet. Das Amtsgeheimnis gilt auch zwischen zwei Ämtern. Der Datenschutzbeauftragte nahm mit dem kantonalen Sozialamt Rücksprache und wies die Gemeinde mangels Vorliegen der gesetzlichen Grundlage für einen Informationsaustausch oder für eine Zweckänderung auf alternative Vorgehensweisen hin. Es könne direkt mit dem Betroffenen das Gespräch gesucht oder eine Neuevaluation der Vermögenslage im Rahmen einer Überprüfung des Anspruchs auf Zusatzleistungen durchgeführt werden. Möglich wäre auch eine Strafanzeige, gestützt auf das Bundesgesetz über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung in Verbindung mit dem Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess.

§ 9 Abs. 1 IDG
Art. 31 Abs. 1 ATSG
Art. 31 ELG
§ 167 GOG

12
Einsatz von Videokameras

Öffentliche Organe und Privatpersonen sind 2014 wiederholt mit Fragen zu Videoüberwachungen an den Datenschutzbeauftragten gelangt. Je nach Art und Zweck der Überwachung respektive des Einsatzes solcher Kameras gelten unterschiedliche Voraussetzungen.

Videokameras können durch öffentliche Organe eingesetzt werden, wenn sowohl der Einsatz solcher Kameras als auch die einzelnen Aspekte der Überwachung verhältnismässig sind. Die Daten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden, die Rahmenbedingungen müssen in einem Reglement festgelegt und auf den Einsatz solcher Kameras muss explizit hingewiesen werden.

Eine Schule wollte ihr Areal mit einer Videoanlage überwachen mit dem Ziel, strafbare Handlungen mittels dieser Aufzeichnungen zu verfolgen. Die von der Schule innerhalb der Hausordnung geregelte Videoüberwachung hielt der datenschutzrechtlichen Überprüfung nicht stand. Die Schule musste aus Transparenzgründen ein Reglement erlassen und wurde darauf hingewiesen, dass die Überwachung zur Verfolgung von strafbaren Handlungen der Polizei vorbehalten ist. Bei Verdacht auf eine Straftat dürfen die Daten zwar

gesichtet, müssen jedoch zur weiteren Auswertung den Strafverfolgungsbehörden übergeben werden. Eine Sichtung darf auch erfolgen, um zivilrechtliche Massnahmen ergreifen zu können. Zudem war keine zeitliche Einschränkung der Überwachung ersichtlich. Haben sich Vandalenakte ausschliesslich ausserhalb des Schulbetriebs ereignet, ist es nicht verhältnismässig, wenn die Videokameras auch während der Schulzeiten in Betrieb sind.

In einem anderen Fall liess eine Gemeinde den lokalen Fernsehsender die Gemeindeversammlung filmen, wobei die Abstimmungen aus den Beiträgen herausgeschnitten wurden. Die Bürgerinnen und Bürger hatten dem Verfahren vorgängig zugestimmt. Eine Privatperson gelangte mit der Frage an den Datenschutzbeauftragten, ob das Vorgehen der Gemeinde rechtmässig sei. Die datenschutzrechtliche Beurteilung ergab, dass Medien grundsätzlich das Recht haben, sich aus öffentlichen Quellen zu informieren. Dieses Recht findet seine Grenzen an überwiegenden öffentlichen und privaten Interessen, beispielsweise beim Persönlichkeitsschutz oder beim Recht auf freie, unbefangene Teilnahme an einer Gemeindeversammlung und der Wahrung des Abstimmungsgeheimnisses. Ob Film- und Tonaufnahmen an einer Gemeindeversammlung zugelassen werden dürfen, ist daher nicht aus der Sicht des Datenschutzes allein, sondern auch im Kontext der Ausübung der Grundrechte zu beantworten. Aus datenschutzrechtlicher Sicht sind geeignete Massnahmen zu treffen, um sicherzustellen, dass keine Abstimmungen aufgenommen werden. Weiter muss jede Person einer Aufnahme der eigenen Voten und Diskussionsbeiträge widersprechen können. Die betroffene Gemeinde verzichtete in der Folge auf Bild- und Tonaufnahmen der Gemeindeversammlungen.

Eine andere Gemeinde wollte in ihrem Hallenbad nebst dem Bassinbereich auch den Eingangs- und Kassenbereich mittels Video überwachen. Der Datenschutzbeauftragte wies die Gemeinde darauf hin, dass keine permanente Überwachung der Mitarbeitenden stattfinden darf. Eine Verhaltensüberwachung der Mitarbeitenden ist aus arbeitsrechtlicher Sicht unzulässig. Auch bei der Überwachung des Eingangs- und Kassenbereichs gilt es, den Verhältnismässigkeitsgrundsatz zu berücksichtigen.

Die Universität Zürich (UZH) wollte mit dem Einsatz von sogenannten Videosupportkameras eine Echtzeitüberwachung von Hörsälen, Seminarräumen und weiteren öffentlich zugänglichen Orten durchführen und reichte dem Datenschutzbeauftragen ein entsprechendes Reglement zur Prüfung ein. Die Kameras sollten unter anderem helfen, bei Störungsmeldungen Massnahmen zu ergreifen, Dozierende bei der Bedienung audiovisueller Geräte zu instruieren und das Übertragen von Vorlesungen in andere Hörsäle sicherzustellen. Zentrales Element bei der Beurteilung war, ob die Rahmenbedingungen derart ausgestaltet waren, dass ein solcher Einsatz als verhältnismässig beurteilt werden konnte. So muss zwischen den einzelnen Zwecken differenziert und die Rahmenbedingungen müssen diesen angepasst werden. Videosupportkameras dürfen zum Einsatz kommen, falls sie nur zu Unterstützungszwecken genutzt werden, falls keine Überwachung von Personen erfolgt, keine Daten gespeichert werden und ihr Einsatz genügend gekennzeichnet ist. Das Reglement der UZH wurde entsprechend angepasst.

§ 8 Abs. 1 IDG
§ 12 IDG
Art. 13 BV
Art. 16 BV
Art. 17 BV
Art. 26 Abs. 1 ArGV 3

13
Datenaustausch Sozialamt/Migrationsamt

Eine Privatperson wandte sich mit der Frage an den Datenschutzbeauftragten, ob der Austausch von Personendaten zwischen dem Sozialamt und dem Migrationsamt ohne Einwilligung und Wissen der betroffenen Person zulässig sei.
Die auf den 1. Januar 2012 in Kraft getretene Änderung des kantonalen Sozialhilfegesetzes (SHG) verpflichtet die Sozialbehörden, den Ausländerbehörden insbesondere folgende Sachverhalte unaufgefordert zu melden: Beginn, Umfang und Beendigung des Bezugs von Sozialhilfe, Rückerstattungen von bezogenen Sozialhilfeleistungen, Umstände, die sich auf die Höhe der Unterstützungsleistung auswirken sowie sonstige Umstände, die für die pflichtgemässe Beurteilung der persönlichen Verhältnisse und den Grad der Integration für die Ausländerbehörde wesentlich sind.
Die Sozialhilfeorgane können andere Tatsachen, die für das ausländerrechtliche Bewilligungsverfahren bedeutsam sein können, der zuständigen Ausländerbehörde unaufgefordert melden. Umgekehrt besteht gemäss SHG eine Verpflichtung von Behörden und Ämtern, bei konkretem Verdacht auf unrechtmässiges Erwirken von Sozialhilfeleistungen Mitteilung an das Sozialamt zu machen. Der Datenschutzbeauftragte kam zum Schluss, dass der Datenaustausch zwischen dem Sozialamt und dem Migrationsamt gestützt auf eine gesetzliche Grundlage erfolgt und damit zulässig ist.

§ § 47a und 47b SHG
§ 16 Abs. 1 lit. a IDG
§ 17 Abs. 1 lit. a IDG

14
Webtracking ohne Google Analytics

Ein öffentliches Organ setzte zur Analyse des Besucherverhaltens seiner Website Google Analytics ein. Ein Bürger wandte sich an den Datenschutzbeauftragten mit der Bitte, dieses Instrument datenschutzrechtlich zu beurteilen und zu veranlassen, dass beim Besuch der Website der Datenschutz gewährleistet ist.
Google Analytics übermittelt die IP-Adresse und weitere Informationen der Websitebesucherinnen und -besucher direkt an die Firma Google in die USA. Google erhält so Kenntnis personenbezogener Daten. Es ist nicht transparent, wie und zu welchen Zwecken diese Informationen ausgewertet und weiter bearbeitet werden. Das öffentliche Organ wies zwar im Impressum auf den Einsatz von Google Analytics hin und nutzte die Funktion zur Anonymisierung der IP-Adresse. Eine Analyse des Datenschutzbeauftragten zeigte aber, dass die IP-Adresse erst nach der Übermittlung an Google anonymisiert wird und es sich somit um eine ausgelagerte Bearbeitung von Personendaten handelt.
Da das öffentliche Organ für die Bearbeitung der Daten verantwortlich bleibt, muss vertraglich sichergestellt werden, dass die Informationen nur zum vorgesehenen Zweck analysiert, von anderen Daten getrennt bearbeitet und nach einer im Voraus definierten Frist gelöscht werden. Weiter müssen die Orte der Datenbearbeitung bekannt und

ein der Schweiz gleichwertiges Datenschutzniveau gewährleistet sein. Das öffentliche Organ konnte mit Google keinen solchen Vertrag abschliessen, weshalb der Einsatz von Google Analytics als nicht datenschutzkonform beurteilt wurde.

Der Datenschutzbeauftragte schlug dem öffentlichen Organ eine alternative Software, wie zum Beispiel Piwik, zur Analyse des Besucherverhaltens vor. Diese speichert die Besucherdaten lokal auf dem Webserver und übermittelt sie nicht an den Hersteller. Das öffentliche Organ hat danach auf die Verwendung von Google Analytics verzichtet.

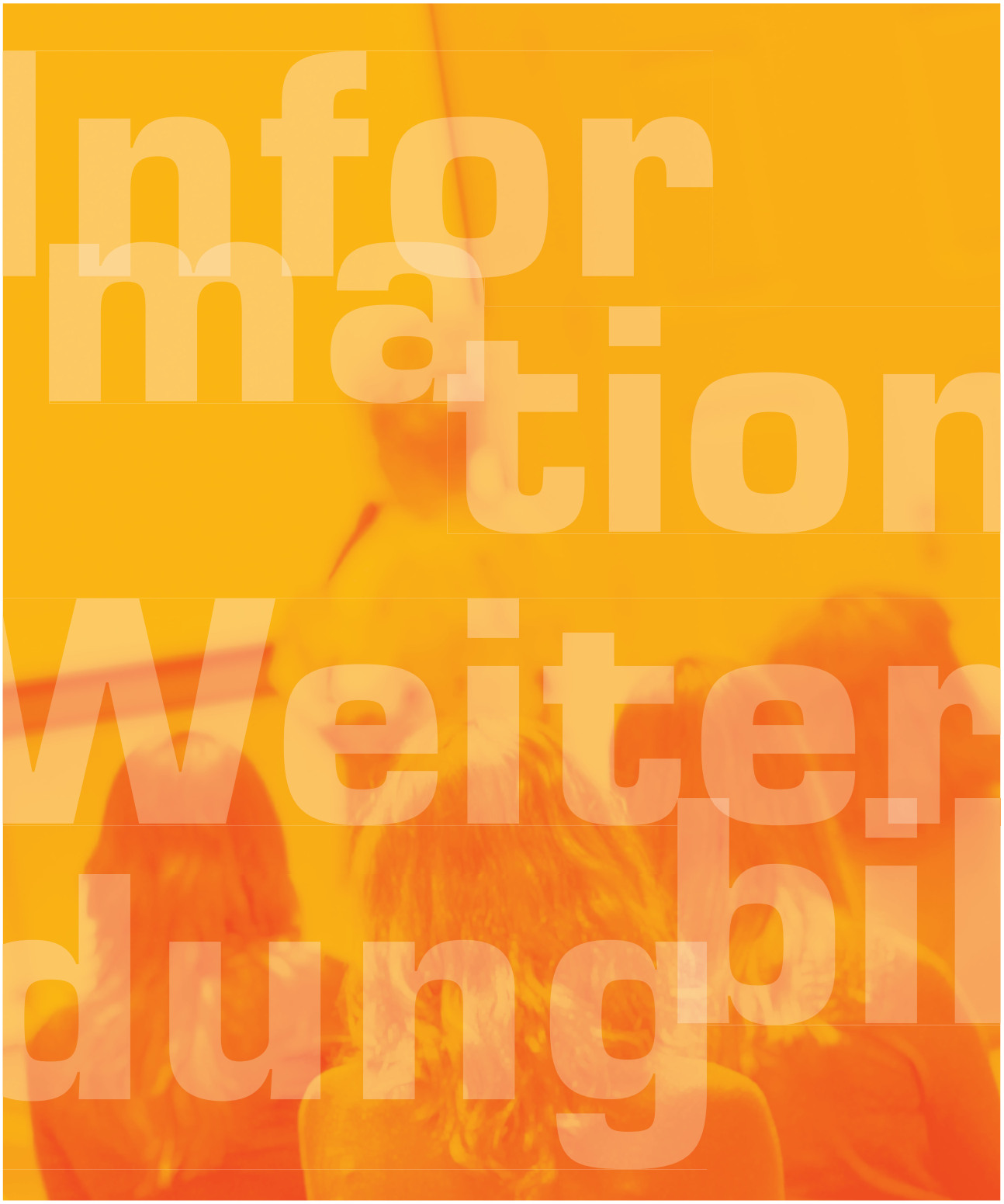
§ 6 IDG
§ 25 IDV
§ 7 IDG

15
Projekt eUmzug

Im Rahmen der E-Government-Aktivitäten lancierte die Staatskanzlei zusammen mit der Direktion der Justiz und des Innern sowie den Städten und Gemeinden des Kantons Zürich das Projekt «eUmzugZH». Ziel des Projekts ist es, die elektronische Abwicklung von Zu-, Weg- und Umzügen zu ermöglichen. Die Projektleitung gelangte an den Datenschutzbeauftragten, um verschiedene datenschutzrechtliche und sicherheitstechnische Fragen bei der Abwicklung von Umzugsmeldungen zu besprechen.
Bei der Einführung einer solchen elektronischen Transaktion entfällt der Behördengang und somit der persönliche Kontakt der Einwohnerinnen und Einwohner mit der Verwaltung, beziehungsweise er wird durch einen elektronischen Austausch ersetzt. An erster Stelle steht daher, dass mit geeigneten Mechanismen die umziehenden Personen eindeutig identifiziert und authentifiziert werden können, um Missbräuche zu verhindern. Dazu wird eine Eingabemaske auf einer Web-Transaktionsplattform zur Verfügung gestellt. Die meldenden Personen müssen durch eine Kombination von verschiedenen zwingenden Eingabefeldern geführt werden, anhand derer die Identifizierung und Authentifizierung erfolgt. Erleichterungen in der Benutzerführung wie zum Beispiel eine Autovervollständigungsfunktion, bei welcher während der Eingabe ein Name oder gar eine Namensliste aus der Einwohnerkontrolldatenbank vorgeschlagen wird, können hier nicht eingesetzt werden. Ebenfalls nicht möglich ist die Umzugsmeldung per E-Mail. Auf diesem Weg kann keine eindeutige Identifikation der umziehenden Person sichergestellt werden. Des Weiteren muss die Datenübermittlung vertraulich sein. Die Transaktion zwischen der meldenden Person und der Gemeinde muss deshalb verschlüsselt erfolgen.

Die notwendigen Massnahmen waren in der Machbarkeitsanalyse der Projektleitung bereits mehrheitlich angedacht beziehungsweise in den vom Bund vorgegebenen Standards für das Vorhaben enthalten. Ab Mitte 2015 soll die gemeindeübergreifende Umzugsmeldung mit einigen Gemeinden in einem Pilotversuch getestet werden.

§ 7 IDG
§§ 32 ff. Gemeindegesetz



«Die Kompetenz im Umgang mit Personendaten muss angesichts des technologischen Wandels gefördert und gefordert werden.»

Den bewussten Umgang mit Daten unterstützen

2014 standen Informationsmittel, die sich direkt an die Bürgerinnen und Bürger wenden, im Zentrum der Kommunikationsarbeit. Die datenschutz.ch-App und die Informationsbroschüre über die individuellen Rechte zum Schutz der Privatsphäre bildeten dabei die beiden wichtigsten Neuerungen.

Unbestrittenes Highlight der Kommunikationsarbeit 2014 des Datenschutzbeauftragten war die Lancierung der ersten interaktiven Datenschutz-App. Ziel der Applikation ist es, den Datenschutz näher an die Userinnen und User von Smartphones und Tablets heranzubringen. Konkret bietet die datenschutz.ch-App folgende Interaktionsmöglichkeiten:

- Möglichkeit, ein Auskunftsgesuch bei einer privaten oder öffentlichen Institution einzureichen
- Passwort-Check zur Beurteilung, ob ein bestimmtes Passwort stark oder schwach ist
- Datenschutz-Reporter zur direkten Übermittlung an den Datenschutzbeauftragten eines Anliegens oder Vorfalls, bei dem möglicherweise der Datenschutz nicht eingehalten oder die Privatsphäre bedroht wird

Darüber hinaus beinhaltet die App Informationen zum Auskunftsrecht sowie über die wichtigsten Rechte im Zusammenhang mit Daten- und Privatsphärenschutz. Das Informationsportfolio wird durch eine Bibliothek mit Fachbeiträgen zu aktuellen datenschutzrechtlichen Fragen ergänzt.

Die App ist sowohl in einer iOS- wie auch in einer Android-Version erhältlich und kostenlos. Seit der Lancierung wurde sie über 6000 Mal heruntergeladen und die Community der Nutzenden wächst stetig.

Symposium debattiert über Snowden und die Folgen

Das 19. Symposium on Privacy and Security der Stiftung für Datenschutz und Informationssicherheit, das traditionsgemäss Ende August stattfand, widmete sich dem Fragenkomplex «Big Data Analytics». Die abschliessende Podiumsdiskussion ging dabei der Frage nach, weshalb die Enthüllungen von Edward Snowden in der Schweiz kaum eine öffentliche Debatte über die zwischenzeitlich fast lückenlose Überwachung der privaten Kommunikationskanäle durch die Geheimdienste ausgelöst hat.

Informationsbroschüre für Bürgerinnen und Bürger

2014 publizierte der Datenschutzbeauftragte die Broschüre «Datenschutz – Meine Rechte». Darin werden die wichtigsten Instrumente erläutert, die den Bürgerinnen und Bürgern zum Schutz ihrer Daten zur Verfügung stehen. Anlass, eine solche Informationsbroschüre zu veröffentlichen, waren die zahlreichen Anfragen zu diesem Themenkomplex, die an den Datenschutzbeauftragten gerichtet werden. Auch stellt die moderne Technologie den Schutz der Privatsphäre und der Persönlichkeitsrechte vor neue Herausforderungen – so wird es immer wichtiger, dass sich die Bürgerinnen und Bürger aktiv vor dem Missbrauch ihrer persönlichen Daten schützen und auch ihre diesbezüglichen Rechte kennen.

Konkret klärt die 16-seitige Publikation in einem ersten Teil über die Grundsätze des Datenschutzes auf. Im zweiten Teil werden die Themen Auskunftsrecht, Datensperre, Recht auf Berichtigung und Vernichtung sowie Recht auf Unterlassung, Beseitigung und Schadenersatz erläutert und es werden Praxistipps zur Einforderung der Rechte präsentiert.

Weiterbildungsangebote mit Qualität

Das Umfeld für Aus- und Weiterbildung hat sich in den vergangenen Jahren stark verändert. Die Anzahl Angebote hat stark zugenommen, gleichzeitig haben sich die Bedürfnisse hin zu individualisierten Lernangeboten verschoben.

Den sich verändernden Rahmenbedingungen begegnet der Datenschutzbeauftragte auf zweierlei Arten: Einerseits sollen die eigenen Weiterbildungsangebote weiterhin hohe Qualität und Verbindlichkeit bieten; wer an einem Kurs teilnimmt, soll Hilfe für den Arbeitsalltag und verlässliche Antworten auf seine Fragen erhalten. Anderseits werden die Angebote laufend modernisiert und den Bedürfnissen angepasst. Der Datenschutzbeauftragte hatte schon vor längerer Zeit ein Lernprogramm «Datenschutz» entwickelt, das im Internet für alle verfügbar ist (Stichwort E-Learning). Dieses Lernprogramm erfreut sich unverändert grosser Beliebtheit. Die Seminarinhalte wurden 2012 überarbeitet (Tätigkeitsbericht 2012, Seite 17).
Zugenommen hat die Nachfrage nach spezifisch auf die Bedürfnisse von einzelnen Anspruchsgruppen zugeschnittenen Kursen, Referaten und Modulen zum Datenschutz.

Evaluation der Seminarangebote

Die Nachfrage nach klassischen Seminaren ist eher rückläufig. Dies hat mehrere Ursachen. Bestimmte Zielgruppen sind über das interne Seminarprogramm des Personalamts schwer erreichbar, wie das Gesundheitspersonal, was zusätzliche Marketingmassnahmen nötig macht. Zeit ist zudem ein knappes Gut: Auch Mitarbeitende öffentlicher Organe müssen Prioritäten setzen und bevorzugen heute eher kurze Weiterbildungs-«Spots» oder längere Weiterbildungen, die mit «Credit Points» (beispielsweise ECTS-Punkte) belohnt werden. Schliesslich möchten die Teilnehmenden auch von Transfereffekten profitieren, indem sie das Gelernte direkt im Arbeitsalltag anwenden können. Dies hat zur Folge, dass die Vor- und Nachbereitung von Seminaren aufwändiger geworden ist, wobei im Gegenzug ihre Wirkung steigt. Während sich die Seminarinhalte bewährt haben, sind Umfang und Form der Angebote zu evaluieren und allenfalls neu zu konzipieren. Künftig soll im Weiterbildungsbereich eng mit der Zürcher Hochschule für angewandte Wissenschaften (ZHAW) zusammengearbeitet werden. Nebst eigenständigen Datenschutz-Kursen sollen auch Module für andere Lehrgänge angeboten werden.

Ausgewählte Referate

- Big Data und Datenschutz
- Privatsphäre in der digitalen Gesellschaft
- Cyber Security – Risiken und Schutz im Internet
- Auskunfts- und Einsichtsrechte von RPK und GPK
- Datenschutz in der klinischen Forschung
- Datenschutz in der sozialen Arbeit

Verhandlungen

«Sensible Datenbearbeitungen müssen auf formell-gesetzlicher Stufe geregelt werden, weil es sich dabei meist um schwere Grundrechtseingriffe handelt.»

Einwohnerregister und sensible Datenbearbeitungen im Fokus

2014 nahm der Datenschutzbeauftragte zu insgesamt elf Gesetzesvorlagen Stellung: Die neuen Erlasse zur Regelung des Bezugs von Einwohnerdaten durch Behörden, Verwaltungsstellen und Gerichte bildeten dabei einen Schwerpunkt.

Ämter und Betriebe der Verwaltung, aber auch Behörden wie Betreibungsämter, Kindes- und Erwachsenenschutzbehörden oder Gerichte haben zunehmend das Bedürfnis, über aktuelle Daten ihrer Kundinnen und Kunden zu verfügen beziehungsweise solche Daten elektronisch abfragen zu können. Dazu bieten sich die Register der Einwohnerkontrollen an. Da es bisher keine kantonale Einwohnerdatensammlung gab, wurden mit der Zeit Hunderte von Online-Zugriffen auf die 169 Gemeinden im Kanton Zürich eingerichtet – eine Vielzahl davon beruhte auf einer dünnen gesetzlichen Legitimation. Im Rahmen der E-Government-Aktivitäten wurden deshalb Anstrengungen unternommen, klare Rechtsgrundlagen für eine kantonale Einwohnerdatenplattform zu schaffen und öffentlichen Organen den Datenbezug über diese Plattform zu ermöglichen. Dazu wurde ein neues Gesetz über das Meldewesen und die Einwohnerregister (MERG) in die Vernehmlassung gegeben (Seite 42).

Ein aktuelles, dringendes Bedürfnis eines Datenbezugs meldete die Gesundheitsdirektion an. Sie wollte zur Prüfung des Wohnsitzes von Spitalpatientinnen und -patienten, für deren stationäre Behandlung der Kanton Kostenanteile übernimmt, rasch eine Möglichkeit zur Abfrage von Einwohnerdaten schaffen. Der Regierungsrat erliess dazu eine Wohnsitzprüfungsverordnung, zu welcher der Datenschutzbeauftragte Stellung genommen hat (Seite 43).

Weitere Anpassungen an Vorgaben des IDG

Sensible Datenbearbeitungen müssen auf formellgesetzlicher Stufe geregelt werden, weil es sich dabei meist um schwere Grundrechtseingriffe handelt. Das IDG sah eine Übergangsfrist zur Umsetzung dieser Anforderung vor. Während die Direktion der Justiz und des Innern und die Bildungsdirektion umfassende Revisionsvorlagen zur Anpassung von Gesetzen in ihrem Bereich erarbeiteten (Tätigkeitsberichte 2012, Seite 36, und 2013, Seite 38), sahen andere Direktionen nur partiellen oder gar keinen Handlungsbedarf für Gesetzesanpassungen. Die Vorlage der Justizdirektion wurde 2014 vom Kantonsrat beschlossen, diejenige der Bildungsdirektion vom Regierungsrat dem Kantonsrat zugeleitet. Auch die Änderungen des Gesetzes über Invalideneinrichtungen für erwachsene Personen und den Transport mobilitätsbehinderter Personen, des Sozialhilfegesetzes (Tätigkeitsbericht 2012, Seite 38) und des Personalgesetzes (Tätigkeitsberichte 2012, Seite 37, und 2013, Seite 29) hat der Kantonsrat verabschiedet. Letztere sind am 1. Mai 2015 in Kraft getreten.

Frühe Einbindung ist wichtig

Gesellschaftliche Veränderungen sowie die immer rasanter verlaufende technologische Entwicklung führen dazu, dass der Gesetzgebungsprozess anspruchsvoller und komplexer geworden ist. Um einen angemessenen Datenschutz sowie entsprechende Informationssicherheitsmassnahmen zu garantieren, ist ein möglichst früher Einbezug des Datenschutzbeauftragten in die Gesetzgebungsarbeiten wünschenswert. Die Möglichkeit, im Rahmen von Mitberichts- und Vernehmlassungsverfahren eine offizielle Stellungnahme abzugeben, ist für den Datenschutzbeauftragten ein wichtiger Pfeiler seiner Tätigkeit.

2014 hat der Datenschutzbeauftragte unter anderem zu folgenden Gesetzgebungsprojekten Position bezogen:

Kanton

- Neuerlass einer Wohnsitzprüfungsverordnung
- Neuerlass eines Gesetzes über das Meldewesen und die Einwohnerregister (MERG)
- Jugendheim- und Familienunterstützungsgesetz (Totalrevision des Jugendheimgesetzes)
- Krebsregistergesetz

Bund

- Änderung des Zivilgesetzbuches (ZGB) im Bereich Adoption
- Änderung des Zivilgesetzbuches (ZGB) im Bereich Kindesschutz
- Parlamentarische Initiative zur Publikation von Erwachsenenschutzmassnahmen
- Bundesgesetz über die Informationssysteme des Bundes im Bereich Sport
- Bundesgesetz über die Geldspiele
- Bundesgesetz über die Informationssicherheit
- Teilrevision des Ausländergesetzes (AuG), des Bundesgesetzes über die Ergänzungsleistungen zur AHV und IV (ELG) und der Verordnung über die Einführung des freien Personenverkehrs (VEP)

Kantonale Einwohnerdatenplattform

2014 wurde der Entwurf für ein Gesetz über das Meldewesen und die Einwohnerregister (MERG) in die Vernehmlassung gegeben. Das Meldewesen und die Einwohnerregister waren bisher im Gemeindegesetz geregelt. Neu soll ein separates Gesetz geschaffen werden. Aus datenschutzrechtlicher Sicht war die Vorlage in ihrer Gesamtheit zu begrüssen, gab aber zu einigen Bemerkungen Anlass.

Die wesentliche Neuerung des MERG ist die Schaffung einer kantonalen Einwohnerdatenplattform (KEP). Die KEP soll die Meldedaten aller Personen enthalten, die sich im Kanton Zürich niedergelassen oder das Aufenthaltsrecht erhalten haben. Dadurch wird eine zentrale Datenbank aller im Kanton Zürich wohnhaften Personen geschaffen. Die KEP wird durch automatisierte Meldungen der Gemeinden, die weiterhin die Einwohnerregister führen, regelmässig aktualisiert.
Mit der Schaffung einer KEP können aktuelle und insbesondere im Rahmen des E-Government absehbare künftige Bedürfnisse der Verwaltung nach aktuellen Einwohnerdaten abgedeckt werden. Dies dient nicht nur der effizienten Verwaltungstätigkeit, sondern unterstützt auch den Grundsatz der Datenrichtigkeit. Aus der KEP sollen sich künftig alle Behörden und Verwaltungsstellen im Kanton Zürich bedienen können, soweit sie die Daten für die Erfüllung ihrer Aufgaben benötigen. Aktuell handelt es sich um rund 200 Amtsstellen, die rund 1,8 Millionen Abfragen pro Jahr tätigen. Im Vollzug bedeutet dies, dass künftig mehrere hundert Verwaltungsmitarbeitende auf einen Datenbestand von über 1,4 Millionen Menschen werden zugreifen können.
Die Bestimmungen über den Datenbezug sahen indessen nur ungenügende Schranken und Sicherungsmechanismen zur Wahrung der Zweckbindung und der Verhältnismässigkeit von Datenbearbeitungen vor. Der Datenschutzbeauftragte forderte deshalb eine grundlegende Überarbeitung des Regelungskonzepts zur KEP. Der darauf überarbeitete Entwurf des MERG hält zwar am Konzept des grundsätzlich offenen Datenbezugs fest, der Regierungsrat soll jedoch auf Verordnungsstufe zusätzliche Schranken und Mechanismen bestimmen, um die Persönlichkeitsrechte der Einwohnerinnen und Einwohner zu wahren. Auch soll eine Liste geführt werden, die sämtliche Datenbezüger und die von ihnen bezogenen Datenkategorien enthält. Eine solche auch vom Datenschutzbeauftragten geforderte Liste, die auch veröffentlicht werden soll, schafft die notwendige Transparenz über die Datenbezüge. Der Regierungsrat beabsichtigt, den Datenschutzbeauftragten in die Ausarbeitung der Verordnung einzubeziehen. In diesem Rahmen werden die konkreten Massnahmen wie die Beschränkung der Zugriffsrechte, die Kontrolle der Zugriffe etc. zu bestimmen sein.

Neue Wohnsitzprüfungsverordnung

Um dem Wohnsitzprinzip bei der Kostenübernahme von stationären Behandlungen in Spitälern Rechnung zu tragen, schickte die Gesundheitsdirektion 2014 einen Verordnungsentwurf für eine Wohnsitzprüfungsdatenbank in die Vernehmlassung. Als problematisch erwies sich dabei vor allem der Vorschlag, die Plattform durch eine externe Stelle zu betreiben.

Der Kanton hat für stationäre Behandlungen in Spitälern Kostenanteile zu tragen. Dabei gilt das Wohnsitzprinzip, das heisst, es hat derjenige Kanton zu zahlen, in welchem die Patientin oder der Patient Wohnsitz hat (Seite 28). Die Gesundheitsdirektion, welche für die Abwicklung der Rechnungen zuständig ist, suchte daher nach Lösungen, um bei jährlich rund 200 000 Rechnungen überprüfen zu können, ob der Kanton zur Kostenübernahme verpflichtet ist. Der Lösungsvorschlag lautete dahingehend, dass der Kanton zwecks Wohnsitzprüfung eine zentrale Datenbank aufbaut, in welcher sämtliche Einwohnerinnen und Einwohner des Kantons erfasst werden. Damit verbunden sollte ein Meldewesen von den Einwohnerkontrollen an die Gesundheitsdirektion eingeführt werden.
Der Datenschutzbeauftragte hatte bereits Ende 2012 anlässlich einer ersten Besprechung dieses Vorschlags Bedenken angemeldet. Diesen wurde insofern Rechnung getragen, als für die Datenbank und die Mutationsmeldungen eine Rechtsgrundlage in Form einer Wohnsitzprüfungsverordnung (WPV) geschaffen werden sollte. Der Verordnungsentwurf wurde dem Datenschutzbeauftragten zur Stellungnahme unterbreitet.
Die Einwohnerregister sind nach geltendem Recht dezentral organisiert und werden von den Gemeinden geführt. Aufgrund dieser Ausgangslage und angesichts der Auswirkungen einer zentralen Einwohnerdatenbank im Kanton Zürich auf die Persönlichkeitsrechte der Einwohnerinnen und Einwohner ist grundsätzlich eine Rechtsgrundlage in Form eines Gesetzes zu fordern (Seite 42). Eine Verordnung reicht aus, wenn sich die Datenbank wie in diesem Fall auf einen bestimmten, konkreten Zweck wie die Prüfung des Wohnsitzes für die Abwicklung von Rechnungen über Hospitalisationen beschränkt und keine sensiblen Personendaten enthält. Bezüglich Zweck der Datenbearbeitung, Inhalte der Datenbank und Datenbekanntgaben von den Gemeinden an die Gesundheitsdirektion genügten die Regelungen der WPV den datenschutzrechtlichen Anforderungen. Ungeklärt waren grundsätzliche Fragen in Bezug auf die Wohnsitzprüfungsdatenbank und ihren Betrieb durch eine andere Verwaltungseinheit ausserhalb der Gesundheitsdirektion (Fachstelle Datenlogistik der Baudirektion). Aufgrund der Hinweise des Datenschutzbeauftragten wurden die Regelungen der Verantwortung und der Auslagerung des Betriebs präzisiert, worauf der Regierungsrat die WPV verabschiedete.
Ungelöst blieb jedoch die vom Datenschutzbeauftragten aufgeworfene grundsätzliche Problematik, dass der Betrieb der Einwohnerdatenbank durch eine Fachstelle der Baudirektion erfolgen sollte. Da kein Sachzusammenhang zwischen dem Betrieb einer kantonalen Einwohnerdatenplattform und den Aufgaben einer Baudirektion besteht, fehlt der Fachstelle die Legitimation, eine solche Aufgabe zu übernehmen.

Gesetz über die Administrativuntersuchung

In seiner Vernehmlassungsantwort begrüsste der Datenschutzbeauftragte die Schaffung von gesetzlichen Bestimmungen zur Administrativuntersuchung. Er wies darauf hin, dass der Zweck von Meldungen der Strafbehörden an die Anstellungs- oder Aufsichtsbehörde klar umschrieben sein muss.

Die Administrativuntersuchung ist ein verwaltungsinternes, aufsichtsrechtliches Verfahren, mit dem ein Sachverhalt innerhalb eines bestimmten Bereichs der Verwaltung vertieft abgeklärt wird. Ziel ist es, die Funktionsfähigkeit und die Integrität der betreffenden Verwaltungseinheit sicherzustellen oder wiederherzustellen.
Bisher fehlten im kantonalen Recht Bestimmungen zur Administrativuntersuchung. Mit dem Gesetz über die Administrativuntersuchung sollen diese geschaffen werden. Mit der Vorlage werden neue Bestimmungen im Gesetz über die Organisation des Regierungsrates und der kantonalen Verwaltung, im Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess, im Lehrpersonalgesetz, im Mittelschulgesetz sowie im Einführungsgesetz zum Bundesgesetz über die Berufsbildung vorgeschlagen.
Der Datenschutzbeauftragte begrüsste in seiner Stellungnahme die Schaffung klarer Regelungen über die Administrativuntersuchung, wies darauf hin, dass die Bestimmungen hinreichend bestimmt sein müssen, und nahm insbesondere zur Änderung des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess Stellung, das die Mitteilungsrechte und -pflichten der Strafbehörden an die Anstellungs- oder Aufsichtsbehörde regelt. Es fehlt in der neuen Bestimmung insbesondere eine Regelung über den Zweck der Meldung. Der Datenschutzbeauftragte kritisierte die Formulierung, die besagt, dass automatisch eine Mitteilung erfolgt, wenn Angestellte ein Verbrechen oder Vergehen begangen haben oder begangen haben sollen, das mit ihrer Tätigkeit nicht vereinbar erscheint.
Die vorgesehene Akteneinsicht der Anstellungs- oder Aufsichtsbehörde ist einerseits an die Bestimmungen der Strafprozessordnung (StPO) anzuknüpfen, die die Akteneinsicht bei hängigen Verfahren regelt und besagt, dass andere Behörden die Akten einsehen können, wenn sie sie für die Bearbeitung hängiger Zivil-, Straf- oder Verwaltungsverfahren benötigen und der Einsichtnahme keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen. Anderseits ist sie als Kann-Vorschrift auszugestalten und von der Eröffnung einer Administrativuntersuchung abhängig zu machen. Einen Anspruch auf Akteneinsicht vorzusehen, ohne dass bereits eine Administrativuntersuchung eingeleitet ist, geht indessen zu weit. Wenn die Anstellungs- oder Aufsichtsbehörde für den Entscheid, ob sie eine Administrativuntersuchung eröffnen soll oder nicht, zusätzliche, über die Mitteilung hinausgehende Informationen benötigt, kann sie über die Amtshilfe Auskünfte einholen.

§ 151 GOG
Art. 101 Abs. 2 StPO
§ 17 IDG

Änderung des Adoptionsrechts im Zivilgesetzbuch

Mit der Revision des Adoptionsrechts des Zivilgesetzbuches und des Partnerschaftsgesetzes sowie weiterer Gesetze sollen die Adoptionsvoraussetzungen und das Adoptionsgeheimnis an die gesellschaftliche Entwicklung angepasst werden. Es soll ausserdem die Stiefkindadoption für eingetragene Paare wie auch für faktische Lebensgemeinschaften geöffnet werden.
Der Datenschutzbeauftragte nahm zu zwei Bestimmungen der Vernehmlassungsvorlage Stellung. Einerseits kam er bezüglich des Adoptionsgeheimnisses zum Schluss, dass Präzisierungsbedarf besteht. Die Regelung, welche die Bekanntgabe von nichtidentifizierenden Informationen über die Lebenssituation des Kindes an die leiblichen Eltern vorsieht, greift erheblich in die Privatsphäre des Kindes und der Adoptiveltern ein. Die Bestimmung sagt nichts über den inhaltlichen und zeitlichen Umfang der Informationspflicht aus. Andererseits hat der Datenschutzbeauftragte in Bezug auf den Anspruch des minderjährigen Kindes auf Auskunft über nichtidentifizierende Informationen über die leiblichen Eltern – als Gegenstück zur Informationspflicht der Adoptiveltern – festgehalten, dass auch hier der sachliche und zeitliche Umfang des Informationsrechts unklar ist.

Art. 268b Abs. 3 VE-ZGB
Art. 268c Abs. 1 VE-ZGB

Totalrevision des Publikationsgesetzes

Der Datenschutzbeauftragte nahm 2014 zur Vorlage über die Totalrevision des Publikationsgesetzes Stellung und wies insbesondere auf den Verhältnismässigkeitsgrundsatz hin.
Vorrangiges Ziel der Totalrevision ist, dass der elektronischen Fassung einer amtlichen Veröffentlichung das Primat zukommen soll. Eine neue Bestimmung sieht vor, dass die Verordnung Zeiträume festlegt, während deren die Veröffentlichungen über eine Suchfunktion erschlossen werden. Neu sollen die Amtsblatt-Ausgaben auch nach Ablauf des Suchzeitraums im Internet abrufbar bleiben.
Gemäss dem Verhältnismässigkeitsprinzip sind öffentliche Bekanntmachungen zu löschen, sobald der Publikationszweck erfüllt ist. Soweit kein überwiegendes öffentliches Interesse an einer unbegrenzten und dauernden Zugänglichkeit von Personendaten über das Internet besteht, ist die Publikationsdauer daher unter Berücksichtigung der divergierenden Interessen zu begrenzen. Bei der Verhältnismässigkeitsprüfung ist zu berücksichtigen, dass Internetpublikationen im Gegensatz zu Papierausgaben weitergehende Möglichkeiten bieten und daher insgesamt eine erhöhte Gefahr für Persönlichkeitsverletzungen mit sich bringen. Dies gilt vor allem für besondere Personendaten. Meldungen, die Personendaten enthalten, sind somit nach einer angemessenen Zeit aus dem Online-Archiv zu löschen. Unter Berücksichtigung, dass das Online-Archiv nicht mit einer Suchfunktion ausgestattet ist und damit das Risiko für eine Persönlichkeitsverletzung minimiert wird, erscheint es angemessen, wenn besondere Personendaten nach einem Jahr und die übrigen Meldungen mit Personenbezug nach drei Jahren aus dem Online-Archiv gelöscht werden.

§ 8 Abs. 1 IDG
§ 20 Abs. 2 VE-PublG

Entwurf eines Bundesgesetzes über die Informationssicherheit

Im März 2014 lancierte der Bundesrat die Vernehmlassung zum neuen Bundesgesetz über die Informationssicherheit (ISG). Damit soll der Thematik der Informationssicherheit in einer Informations- und Wissensgesellschaft erstmals angemessen Rechnung getragen werden. Auch schliesst das ISG hinsichtlich Personensicherheitsprüfungen eine Gesetzeslücke, da die damit verbundenen schweren Eingriffe in die Persönlichkeitsrechte einer formell-gesetzlichen Grundlage bedürfen.

In seiner Stellungnahme begrüsste der Datenschutzbeauftragte die Schaffung klarer Regelungen im Bereich der Informationssicherheit und unterbreitete verschiedene Ergänzungsvorschläge.

Neben der Wahrung der Eigeninteressen des Bundes im Bereich der Informationssicherheit sollten die verfassungsmässig garantierten Persönlichkeitsrechte sowie die Berufs-, Geschäfts- und Fabrikationsgeheimnisse ebenfalls direkt durch das ISG geschützt werden. Der DSB schlug daher eine entsprechende Ergänzung des Zweckartikels vor.

Während die Pflicht, in bestimmten Fällen ein Informationssicherheitskonzept zu erstellen, durch den DSB klar begrüsst wird, regt er bezüglich der vorgeschlagenen Standardanforderungen und -massnahmen zur Informationssicherheit, die lediglich empfehlenden Charakter haben sollen, an, diese generell für sämtliche dem ISG unterworfenen Behörden und Organisationen verbindlich zu erklären.

In den Geltungsbereich des ISG fallen auch diejenigen kantonalen Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsrelevante Tätigkeiten ausüben. Diese Regelung greift zwar in die Organisationsautonomie der Kantone ein, ist von der Sache her aber sinnvoll, da nur so die durchgängige Sicherheit von Informationen im ganzen Verantwortungsbereich des Bundes gewährleistet werden kann. Daraus ergibt sich für die Kantone, und allenfalls auch die Gemeinden, die Notwendigkeit, ihre eigenen Informationssicherheitsregeln an das ISG anzupassen. Der Datenschutzbeauftragte empfahl deshalb in seiner Vernehmlassungsantwort, dass den betroffenen Kantonen und Gemeinden die Möglichkeit eröffnet wird, die entsprechenden Informationssicherheitsdienstleistungen der Bundesfachstellen in Anspruch zu nehmen.

Das neue ISG erlaubt auch die Bearbeitung von Personendaten zur Abwehr von Gefahren, ohne dass dies für die betroffenen Personen ersichtlich ist. Dieses Vorgehen lässt sich aus Sicht des Privatsphärenschutzes nur dann rechtfertigen, wenn nach dem Wegfall der vermuteten Gefahr – analog zum Vorgehen bei Observationen, verdeckten Ermittlungen oder verdeckter Fahndung gemäss Strafprozessordnung – eine Mitteilung an die betroffene Person erfolgt. Der DSB verlangte deshalb eine entsprechende Ergänzung des Gesetzestextes.

Zur Frage der Organisation des Datenschutzes unterstrich der DSB, dass die Datenschutzaufsicht über die kantonalen Behörden, die im Auftrag des Bundes sicherheitsrelevante Tätigkeiten ausüben, bei den kantonalen Datenschutzbeauftragten bleiben muss. Kantonale öffentliche Organe werden beim Vollzug von Bundesaufgaben nicht zu Bundesorganen und bleiben deshalb dem kantonalen (Informations- und) Datenschutzgesetz und der kantonalen Datenschutzaufsicht unterstellt.

Der Datenschutzbeauftragte empfahl deshalb eine Ergänzung des Gesetzestextes, wonach der Bundesrat diese durch kantonale Organe im Auftrag des Bundes durchgeführten sicherheitsrelevanten Tätigkeiten in einer Verordnung festzulegen hat.

Art. 1 E-ISG
Art. 10 Abs. 2 und Art. 13 Abs. 2 BV
Art. 23 E-ISG

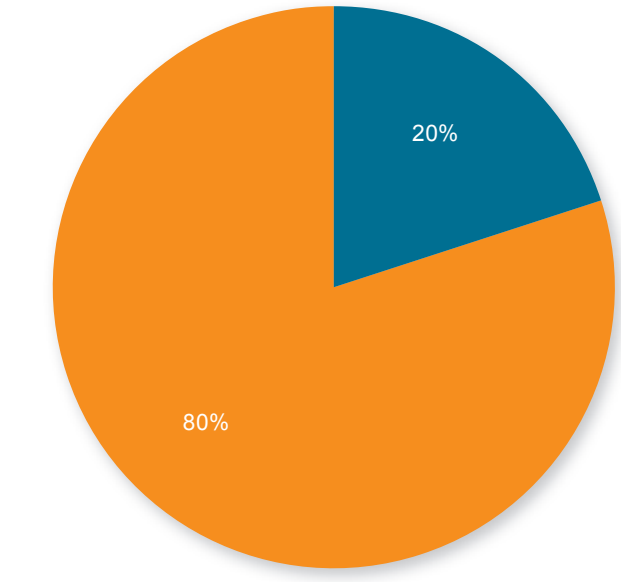
«Kontrollen beziehen sich nicht nur auf den Umgang des öffentlichen Organs mit Personendaten, sondern auch auf den korrekten Umgang des öffentlichen Organs mit den Rechtsansprüchen einzelner Gesuchsteller.»

Überprüfung der Websites von Schulen

2014 überprüfte der Datenschutzbeauftragte, ob die Websites von Schulen Sicherheitslücken aufweisen und ob die in die Websites eingebunden Produkte datenschutzkonform eingesetzt werden. Ein Grossteil der Websites musste beanstandet werden.

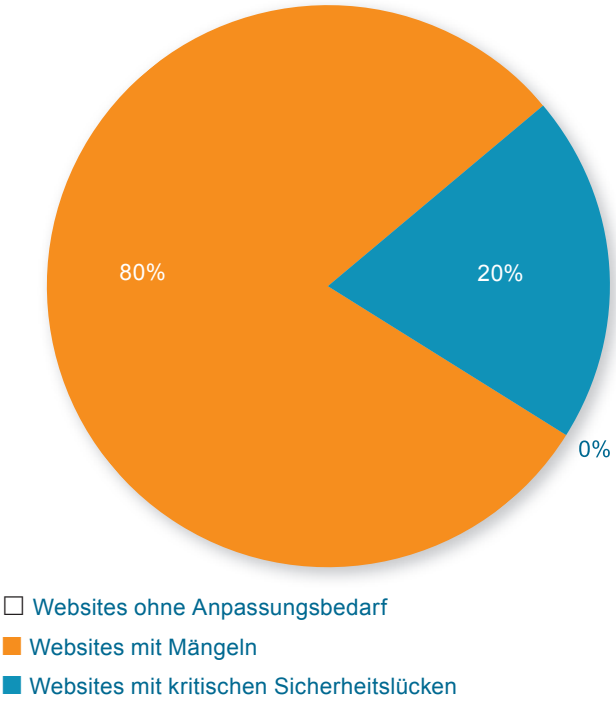
Im Rahmen seiner Reviews stellte der Datenschutzbeauftragte fest, dass die Websites von öffentlichen Organen oft Schwachstellen und Sicherheitslücken aufweisen. Diese waren mehr oder weniger gravierend. Aus diesem Grund erfolgte eine systematische Überprüfung von Schulwebsites. Dabei wurden risikobasiert die Websites von zehn Schulen ausgewählt und einer Überprüfung unterzogen. Da die Websites oft von einem externen Partner betrieben werden, musste dieser bei der Kontrolle einbezogen werden. Es stellte sich heraus, dass viele Schulen Drittdienste, beispielsweise Google Maps, nicht datenschutzkonform einsetzten. Bei 80 Prozent der Schulen waren Programmcodes der Firma Google in die Website eingebunden. Dadurch wurden Informationen der Besucherinnen und Besucher der Website an Google in die USA übermittelt. Ein schriftlicher Vertrag, der insbesondere den Umgang mit Personendaten betreffend Verantwortung, Verfügungsmacht und Zweckbindung, aber auch Geheimhaltungsverpflichtungen, Sicherheitsmassnahmen sowie Kontrollen und die Löschung der Daten regelt, fehlte in allen Fällen. Ausserdem kamen bei allen Websites Sicherheitslücken zum Vorschein. Eine Schulwebsite enthielt eine kritische Sicherheitslücke, wodurch der Inhalt der Website verändert werden konnte. Es wäre ohne weiteres möglich gewesen, Malware über die Website zu verbreiten. Bei einer anderen Schule war die Administrationswebsite ohne Passwort zugänglich, wodurch ebenfalls der Inhalt verändert werden konnte.
Die zwei folgenden Grafiken geben einen Überblick über die Resultate der Überprüfungen.

Einbindung von Diensten Dritter in Schulwebsites



Der Datenschutzbeauftragte forderte die Schulen auf, Drittdienste datenschutzkonform einzusetzen und die Schwachstellen zu beheben. Aufgrund der hohen Anzahl an Mängeln wird der Datenschutzbeauftragte weitere Schulwebsites überprüfen.

Schwachstellen auf Websites



E-Recruiting im Personalwesen

Eine Direktion plante die Einführung einer Software für die Online-Rekrutierung (E-Recruiting). Damit sollte der Personalgewinnungsprozess effizienter gestaltet werden. Die Direktion bat den Datenschutzbeauftragten um eine Vorabkontrolle.
Mit dieser Software wird grundsätzlich keine neue Datenbearbeitung geplant, einzig die Bearbeitungsart ändert sich. Infolgedessen wurde die Vorabkontrolle auf das Erfordernis einer hinreichend bestimmten Rechtsgrundlage, die Zweckgebundenheit und die Informationssicherheitsmassnahmen beschränkt.

Das Personalgesetz äussert sich nur begrenzt zur elektronischen Bearbeitung von Bewerbungen. Es hält einzig fest, dass die Bestimmungen über Personalakten und -dossiers sowie über die Beschaffung, Bekanntgabe und Aufbewahrung von Personendaten auch für elektronisch geführte Datensammlungen gelten. Mit Blick auf die Tatsache, dass aus dem Projektantrag keine neuen Datenbearbeitungen ersichtlich waren und dass Bestimmungen für eine kantonale E-Recruiting Plattform in der Personalgesetzrevision vorgesehen sind, steht dem Einsatz des elektronischen Bewerbungsverfahrens nichts entgegen. Es muss jedoch sichergestellt werden, dass die erhobenen Bewerbungsdaten nur im Rahmen des festgelegten Prozesses bearbeitet werden. Zum Schutz der Daten sind angemessene Informationssicherheitsmassnahmen zu implementieren. Sollten mit dieser Software andere, nicht im Projekt enthaltene Datenbearbeitungen in Betracht gezogen werden, würden diese einer neuen Vorabkontrolle unterliegen.

§§ 7, 9, 10 IDG
§ 34 Abs. 1 PG
§ 23 VVO

E-Government-Dienstleistungen im Steuerbereich

Eine Gemeinde beabsichtigte, verschiedene Dienstleistungen im Rahmen des E-Government einzuführen. Es handelte sich um die Dienste eSchKG (elektronische Übermittlung von Betreibungsbegehren an die Betreibungsämter), E-Rechnung (elektronische Zustellung von Steuerrechnungen und Verfügungen an die Steuerpflichtigen) und E-Konto (Online-Steuerkonto der Steuerpflichtigen zur Übersicht über die eigenen Debitorendaten, die erhaltenen Rechnungen und bezahlten Beiträge sowie zur Generierung von Einzahlungsscheinen für die jeweilige Steuerperiode). Die Gemeinde bat den Datenschutzbeauftragten um eine Vorabkontrolle.

Die datenschutzrechtliche Prüfung ergab, dass für Datenbearbeitungen im Rahmen von eSchKG und E-Rechnung bereits bundes- respektive kantonalrechtliche Grundlagen bestehen. Somit erübrigte sich eine weitere Beurteilung dieser Vorhaben.

Bei der Einführung des E-Konto handelt es sich um ein neues Instrument – jedoch nicht um eine neue Datenbearbeitung –, welches den Bürgerinnen und Bürgern erlaubt, Informationen zu ihren Steuern elektronisch abzurufen und teilweise auch zu bearbeiten. Die Bearbeitung der Informationen kann deshalb auf bestehendes kantonales Recht abgestützt werden. Aufgrund des elektronischen, über das Internet stattfindenden Prozesses muss jedoch sichergestellt werden, dass angemessene technische und organisatorische Informationssicherheitsmassnahmen umgesetzt werden.

§ 7 IDG
§ 8 Abs. 1 IDG
§ 109c Abs. 1 StG
§ 122 StG
§ 173 StG
§ 46 VO StG
§ 6 Abs. 1 Verordnung über die elektronische Zustellung von Verfügungen und Rechnungen
Art. 33a SchKG
Art. 14 VeÜ-ZSSV
Art. 1–5 und 7 Verordnung über die elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs

Impressum

Herausgeber: Datenschutzbeauftragter des Kantons Zürich, Postfach, 8090 Zürich
Lektorat: Text Control, Im Struppen 11, 8048 Zürich
Layout: René Habermacher, Visuelle Gestaltung, Flurstrasse 50, 8048 Zürich
Druck: Kantonale Drucksachen & Materialienzentrale (kdmz), Zürich
Auflage: 900

ISSN 1422-5816

Kontakt

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

dsb

datenschutzbeauftragter
kanton zürich

www.datenschutz.ch

Datenschutz mit Qualität