dsb

datenschutzbeauftragter
kanton zürich

2012

Tätigkeitsbericht

Datenschutzbeauftragter Kanton Zürich

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

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

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

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

«Die Vermittlung von Know-how zu Datenschutz und Privatheit ist auch ein Bildungsauftrag.»

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 2012 bis und mit 31. Dezember 2012 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, März 2013

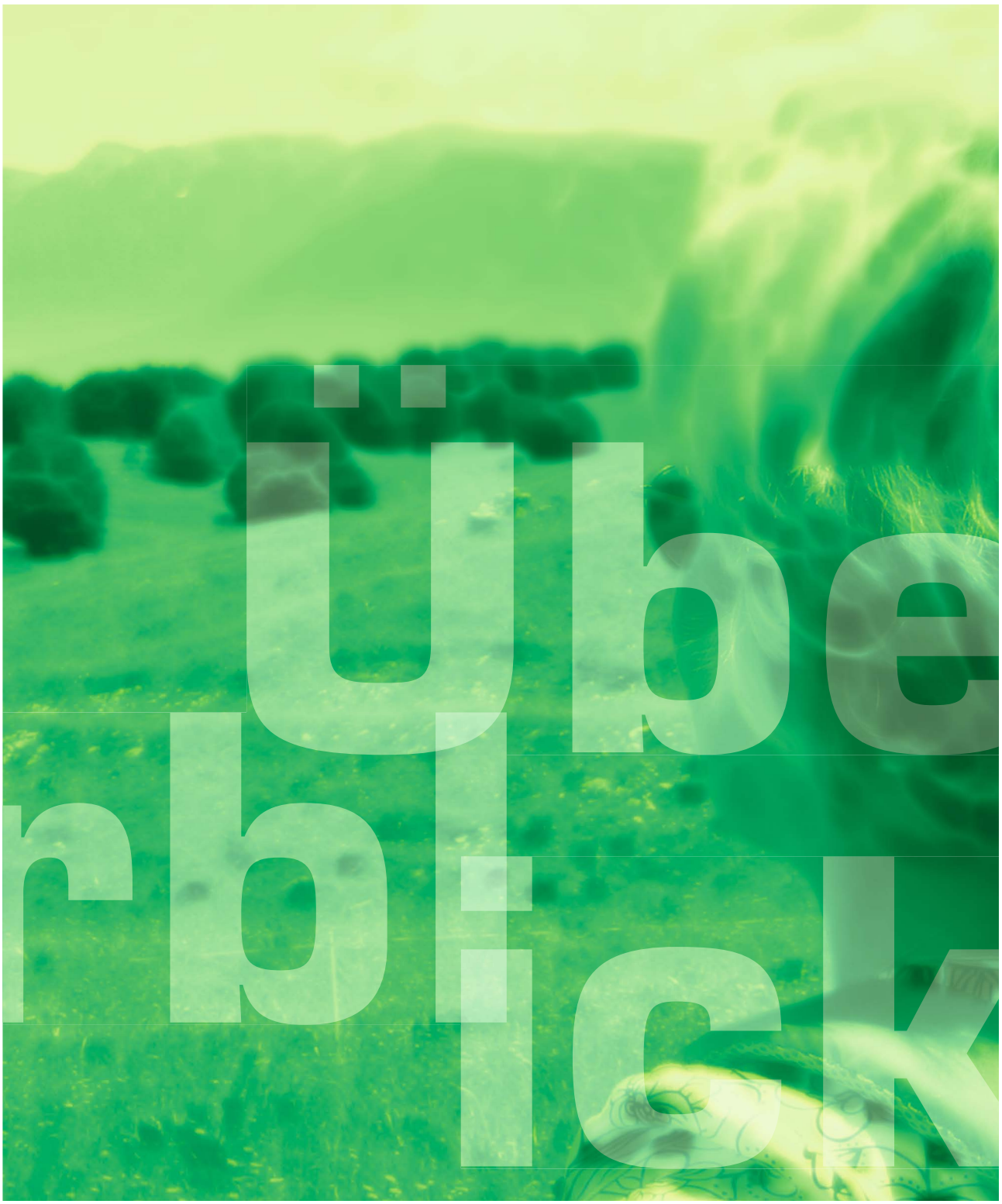
Der Datenschutzbeauftragte des Kantons Zürich
Dr. Bruno Baeriswyl

Überblick

Beratung

Vernehmlassungen

Kontrollen und Vorabkontrollen



Überblick

«Die Nutzung von Daten wird immer intensiver. Die Anforderungen und der Aufwand für den Schutz und die Sicherheit der Daten nehmen zu.»

Daten nutzen und schützen

Die Nutzung von Daten wird immer intensiver. Dies zeigt sich auch am zunehmenden Aufwand für den Schutz der Daten.

Die umfassende Nutzung von Daten ist in der modernen Verwaltung zur Selbstverständlichkeit geworden. Nicht nur werden bestehende Datenbestände intensiver genutzt, sondern neue gesetzliche Grundlagen erlauben auch die Ausweitung der Datenbearbeitungen. Dies ist auch spürbar in der Beratungstätigkeit des Datenschutzbeauftragten: Je umfangreicher die Datenbearbeitungen werden, desto häufiger stellen sich Fragen des Datenschutzes und der Informationssicherheit.

Einbezug des Datenschutzbeauftragten

Für viele Verwaltungsstellen ist es deshalb selbstverständlich geworden, den Datenschutzbeauftragten frühzeitig in die Projekte einzubeziehen. Dank der guten Zusammenarbeit ist es jeweils möglich, adäquate Lösungen für den Datenschutz und die Informationssicherheit zu finden. Diese Beratungen machen einen grossen Teil der Tätigkeiten des Datenschutzbeauftragten aus. Sie sind aufwändig, bedeuten aber einen nachhaltigen Einsatz für den Schutz der Privatsphäre der Bürgerinnen und Bürger.

Datenschutz und Informationssicherheit sind insbesondere bei strukturellen Projekten wie der systematischen Auslagerung von Datenbearbeitungen (siehe auch Seiten 8 bis 9) oder bei umfassenden elektronischen Abwicklungen von Datentransfers zwischen Bürgerinnen und Bürgern und der Verwaltung wie beispielsweise bei der elektronischen Steuererklärung zu beachten. Es zeigt sich, dass das Vertrauen in solche Lösungen nur gewonnen werden kann, wenn die Bürgerinnen und Bürger sich auf die Umsetzung des Datenschutzes und der Massnahmen zur Datensicherheit verlassen können. Der Datenschutzbeauftragte wirkt mit seinen Beratungen und Kontrollen auch vertrauensbildend. Wenn Verwaltungsstellen in Medienmitteilungen ihr Projekt mit der Bemerkung «mit dem Datenschutzbeauftragten abgesprochen» lancieren, sind sie sich bewusst, dass sie damit auch eine klare Verpflichtung gegenüber den Bürgerinnen und Bürgern eingehen.

Kontrollen sind notwendig

Um das Vertrauen der Bürgerinnen und Bürger tatsächlich zu erhalten, sind auch regelmässige Kontrollen des Datenschutzbeauftragten notwendig. Auch diese Kontrolltätigkeit ist in den letzten Jahren aufgrund komplexerer Datenbearbeitungen aufwändiger geworden (siehe auch Seite 40). Zahlreiche Verwaltungsstellen begrüssen die Kontrollen, da diese immer mit einer Reihe von Vorschlägen für eine Verbesserung des Datenschutzes und der Informationssicherheit einhergehen. Insbesondere Gemeinden, die selber über wenig Know-how in diesem Bereich verfügen, geben sehr positives Feedback.

Allerdings ist es auch im letzten Jahr vorgekommen, dass Kontrollen bei einzelnen Verwaltungsstellen anfänglich auf Ablehnung gestossen sind. Dabei wurden einerseits formale Gründe vorge-

bracht – beispielsweise wurde die Zuständigkeit des Datenschutzbeauftragten bei einem privatrechtlich organisierten Regionalspital bestritten oder der Beizug von externen Fachleuten für die Kontrolle wurde in Frage gestellt. In allen Fällen konnten die Kontrollen nach einer Klärung der Situation durchgeführt werden, aber es bleibt ein ungutes Gefühl zurück, da die Einwände von Beginn weg nicht stichhaltig waren und Termine für die Kontrolltätigkeit nicht gewährt wurden. In Bezug auf das Vertrauen in die Datenbearbeitungen dieser Organe ist ein solches Verhalten nicht förderlich.

Datenschutz als Selbstverständnis

Dass die Beachtung des Datenschutzes für viele öffentliche Organe zu einer Selbstverständlichkeit geworden ist, bedeutet nicht, dass Anstrengungen für die Gewährleistung des Datenschutzes und der Informationssicherheit nicht weiterhin notwendig wären. Im Gegenteil: Wie die ständigen Medienmitteilungen über Cyber-Attacken zeigen, muss der Sicherheit der Daten hohe Aufmerksamkeit geschenkt werden. Ein angemessener Sicherheitsstandard kann aber nur erreicht werden, wenn die getroffenen Sicherheitsmassnahmen regelmässig überprüft werden. Die Kontrollen des Datenschutzbeauftragten tragen dazu bei, hier auf fehlende Massnahmen und gesteigerte Anforderungen hinzuweisen.

Auch die Nutzung von neuen Kommunikationsmöglichkeiten wie sozialen Medien beinhaltet zahlreiche Herausforderungen für den Schutz der Privatsphäre der Bürgerinnen und Bürger. Hierzu hat der Datenschutzbeauftragte die öffentlichen Organe beraten und insbesondere im Rahmen von Ausbildungstätigkeiten auf den korrekten Umgang mit persönlichen Daten in diesem Umfeld hingewiesen (siehe Seiten 18 bis 21).

Der Schutz der Privatsphäre wird weiterhin ein wesentliches Anliegen unserer liberalen Gesellschaft bleiben müssen, dies umso mehr, als die neuen technologischen Entwicklungen noch grössere Herausforderungen bringen werden (siehe Seite 14).

Weitere Schwerpunkte

- Datenschutz im Schulbereich
- Auslagerung von Datenbearbeitungen
- Publikation amtlicher Informationen im Internet
- Informationssicherheit in Institutionen mit öffentlichem Auftrag

Auslagerung von Datenbearbeitungen mit neuen Risiken

Durch Cloud Computing wird Outsourcing immer einfacher. Vielfach gehen dabei die datenschutzrechtlichen Anforderungen an die externe Datenhaltung vergessen. Die Verantwortung für die Datenbearbeitung kann nicht ausgelagert werden.

Die Anforderungen an die Auslagerung von Informatikleistungen waren 2012 immer wieder Thema der Beratung durch den Datenschutzbeauftragten. Dies ist nicht zuletzt der auch im Verwaltungsbereich zunehmenden Nutzung von Cloud-Services zuzuschreiben.

Jeder Auslagerung liegt die Tatsache zugrunde, dass die Verantwortung für die Daten und deren Bearbeitung nicht an Dritte übertragen werden kann. Diese ist und bleibt beim auslagernden öffentlichen Organ. Dabei ist es unwesentlich, wo die Daten gespeichert sind und ob ein Cloud-Service in Anspruch genommen wird oder nicht. Gemäss IDG muss ein schriftlicher Vertrag mit dem Auftragnehmer vorliegen. Darin müssen mindestens Gegenstand und Umfang der übertragenen Aufgaben, der Umgang mit Personendaten, die Geheimhaltungsverpflichtungen, die Behandlung von Informationszugangsgesuchen, die Schutzmassnahmen, die Kontrollen, die Sanktionen, die Vertragsdauer und die Kündigungskonditionen geregelt werden. Inhalt und Umfang der Vertragsbestimmungen richten sich massgeblich nach der Art der Daten, deren Sensitivität sowie nach der Art der in Anspruch genommenen Leistungen.

Als weitere Voraussetzung gilt, dass einer solchen Datenbearbeitung durch Dritte keine rechtlichen oder vertraglichen Bestimmungen entgegenstehen dürfen. Es ist zu prüfen, ob die Daten besonderen Geheimhaltungspflichten wie dem Amts- oder Berufsgeheimnis unterliegen. Wenn ja, sind insbesondere beim Berufsgeheimnis Massnahmen wie beispielsweise die Unterstellung der Mitarbeitenden des Auftragnehmers unter das Weisungsrecht des Auftraggebers zu vereinbaren.

Je sensibler die Daten, desto strikter die Schutzmassnahmen

Im Weiteren sind der Sensibilität der Daten angepasste Massnahmen vertraglich festzuhalten. Diese müssen die Vertraulichkeit, die Integrität und die Verfügbarkeit gewährleisten. Dazu ist eine Risikoanalyse durchzuführen. Je nach Resultat derselben können beispielsweise eine Verschlüsselung, die Protokollierung der Zugriffe inklusive regelmässiger Kontrollen, eine strikte Mandantentrennung, eine starke Authentifizierung (beispielsweise Chipkarte mit PIN), redundante Komponenten, Richtlinien und Schulungen für die Benutzenden adäquate Massnahmen zum Schutz der Daten sein.

Wird die Datenbearbeitung ins Ausland verlagert, so sind auch hier die den entsprechend höheren Risiken angepassten Vorkehrungen zu treffen. Es ist zu prüfen, ob der ausländische Staat ein im Vergleich zur Schweiz gleichwertiges Datenschutzniveau aufweist.

Spezielle Vorkehrungen in der Cloud

Werden die Daten in eine Cloud ausgelagert, so müssen die Massnahmen zusätzlich an die einer Cloud inhärenten Risiken angepasst werden. Dabei ist vor allem an die verteilte Datenhaltung mit den unterschiedlichsten zugriffsberechtigten Personen und dem orts- und geräteunabhängigen Zugriff zu denken. Im Vertrag ist folglich detailliert und schriftlich festzuhalten, wer wofür im Sinne des IDG verantwortlich zeichnet. Die Kontrollrechte des öffentlichen Organs sowie unabhängiger Aufsichtsbehörden sind zu verankern. Der Cloud-Anbieter ist zu verpflichten, regelmässig Kontrollen nach internationalen Standards durchführen zu lassen. Weitere Bestimmungen in Bezug auf die Gewährleistung der Rechte betroffener Personen auf Berichtigung und Löschung, aber auch über die Orte der Datenbearbeitung sind aufzunehmen. Festzuhalten ist auch, dass Unterauftragsverhältnisse offengelegt und nur mit Zustimmung des öffentlichen Organs vereinbart werden dürfen. Das anwendbare Recht und der Gerichtsstand sind zu vereinbaren. Um sich mit dem Thema Cloud Computing vertraut zu machen, finden sich detaillierte Ausführungen im Merkblatt «Cloud Computing», publiziert auf der Website des Datenschutzbeauftragten.

Ein umfassender und der Sensitivität der Daten angepasster Vertrag gibt zwar einen gewissen Schutz bei der Durchsetzung allfälliger Vertrags- oder Persönlichkeitsverletzungen. Wichtiger noch als die Vertragsgestaltung ist jedoch die Umsetzung der Massnahmen und deren laufende Überprüfung.

Massgeschneiderte Allgemeine Geschäftsbedingungen fürs Outsourcing

Die datenschutzrechtlichen Anforderungen bei einer Inanspruchnahme von Informatikleistungen unter Beizug von Dritten sind in den «Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen» zusammengefasst. Diese sind als Vertragsbestandteil gedacht und ermöglichen eine umfassende und korrekte Berücksichtigung der datenschutzrelevanten Aspekte beim Abschluss eines Vertrages.

Zusammenfassend kann festgehalten werden, dass bei einer Auslagerung beispielsweise eines Maildienstes, der Inanspruchnahme einer Textverarbeitung oder einer Dateiablage die richtigen Fragen gestellt und auch klar beantwortet werden müssen. Namentlich soll man sich fragen, welche Daten bearbeitet werden, wo und wer sie bearbeitet, wie hoch ihr Schutzbedarf ist, wie sie geschützt werden und wer darauf Zugriff hat. Werden die zum Schutz der Daten erforderlichen Massnahmen geregelt und deren Umsetzung regelmässig kontrolliert, steht aus datenschutzrechtlicher Sicht einer Auslagerung nichts entgegen.

§ 6 IDG
§ 25 IDV
§ 7 IDG

Umgang mit der Privatsphäre gehört zur Medienkompetenz

Die Nutzung sozialer Medien wie Facebook, Twitter und YouTube ist heute selbstverständlich – auch in und rund um die Schule. Das Bewusstsein in Bezug auf die Privatheit, das Know-how über den datenschutzfreundlichen Umgang mit den eigenen Daten und Kenntnisse über die konkreten Privacy-Einstellungen sollten ebenso selbstverständlich sein. Dies ist auch ein Bildungsauftrag.

Kinder werden bereits im Vorschulalter mit elektronischen Gadgets konfrontiert und in der Primarschule mit Tablets ausgerüstet. Damit steht auch die Schule in der Pflicht, wenn es darum geht, den Schülerinnen und Schülern einen bewussten und verantwortungsvollen Umgang mit den persönlichen Daten zu vermitteln.

Omnipräsente soziale Netzwerke erfordern neues Know-how

Soziale Medien werden heute permanent und überall benutzt; sie sind integraler Bestandteil unseres Alltags geworden. Datenschutz und Medienkompetenz stehen im Zentrum, wenn es um den Schutz der Privatsphäre und somit um den Schutz der persönlichen Daten geht. Sind die Daten einmal im Netz, so unterliegen sie – im Vergleich zu einer konventionellen Veröffentlichung beispielsweise in gedruckter Form – ungleich grösseren Risiken in Bezug auf eine Weiterverwendung, die auch missbräuchlich sein kann. Der Datenschutzbeauftragte hat aus diesen Gründen das Projekt «Datenschutz in der Schule» ins Leben gerufen. Ziel dieses Vorhabens ist es, im Bereich der Schulen möglichst viele Personen mit dem Thema Datenschutz und Medienkompetenz zu erreichen und auf mögliche Risiken aufmerksam zu machen. Dazu sollen einerseits Schulleitungen und Lehrpersonen informiert und sensibilisiert werden. Kenntnisse über die Grundlagen des Datenschutzes, der Umgang mit den Schuldaten, aber auch beispielsweise die datenschutzkonforme Inanspruchnahme sozialer Medien und moderner Webdienste wie Cloud Computing werden immer wichtiger. Andererseits sollen auch die Schülerinnen und Schüler im Umgang mit ihren eigenen Daten in Bezug auf ihre Persönlichkeitsrechte und die Privatsphäre sensibilisiert werden. Botschaften wie «Meine Daten gehören mir», «Ich werde möglichst wenig persönliche Informationen im Netz preisgeben» und «Ich muss immer meine Privacy-Einstellungen vornehmen» sollten jede Schülerin und jeder Schüler kennen.

Mittel- und Berufsschulen im Fokus

Der Lancierung des Projekts «Datenschutz in der Schule» ging eine vertiefte Analyse der aktuellen Herausforderungen und Anspruchsgruppen im Bereich Ausbildung voraus. Diese ermöglichte

eine Bestimmung der Zielgruppen und der Schwerpunkte des Vorhabens.
In einem ersten Schritt werden daher auf der Sekundarstufe II (Mittel- und Berufsschule) möglichst viele Stakeholder mit dem Thema Datenschutz und Medienkompetenz angesprochen. Dazu wurde mit der Kantonsschule Stadelhofen ein Pilotprojekt durchgeführt und anlässlich einer Weiterbildungsveranstaltung für Lehrpersonen ein Workshop zum Thema Medienkompetenz angeboten. Dabei wurden anhand konkreter Beispiele die Entstehung und die Grundlagen des Datenschutzes ebenso thematisiert wie die Risiken und Massnahmen zum Schutz von Privatsphäre und Persönlichkeitsrechten.

Kantonsschülerinnen und -schüler diskutieren über Facebook & Co

Weiter fand am europäischen Datenschutztag eine auch für die Medien zugängliche Schulstunde an der Kantonsschule Stadelhofen statt; die Gesprächsrunde wurde im Rahmen einer ordentlichen Lektion zum Thema Medienkompetenz durchgeführt. Neben einer Einführung zur Funktionsweise und zu den damit verbundenen Risiken von sozialen Netzwerken bei der Bekanntgabe von persönlichen Informationen beinhaltete die Präsentation auch eine Live-Demonstration zur optimalen Auswahl der Privatsphäre-Einstellungen bei Facebook, die von den Schülerinnen und Schülern unmittelbar bei ihrem jeweiligen Account umgesetzt werden konnten. Im Anschluss an die Lektion gab der Datenschutzbeauftragte eine Checkliste mit den empfohlenen Privacy-Einstellungen bei Facebook ab.

Schule bleibt ein Thema

Beabsichtigt ist eine umfassende Verankerung der Vermittlung von Know-how zu Datenschutz und Privatsphäre im Schulalltag und in den Lehrmitteln. Die Thematik wird auch in den kommenden Jahren Teil der Tätigkeit des Datenschutzbeauftragten sein, sei dies durch die Zusammenarbeit mit den für den Schulbereich Verantwortlichen, durch das Zurverfügungstellen von Informationen mittels Leitfäden, Merkblättern und Checklisten, durch Beratung bei rechtlichen und technischen Fragen oder durch die konkrete Vermittlung von Wissen.

Etappenweise Evaluation

Die Wirkung des Informations- und Datenschutzgesetzes (IDG) wird in Zukunft mit jährlich wechselnden Schwerpunkten gemessen werden.

Das von der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) erstellte Konzept zur Messung der Wirkung des IDG schlägt vor, dass jährlich jeweils ein anderer der Wirkung evaluiert wird und dass nach einer bestimmten Zeit eine Gesamtevaluation unter Berücksichtigung der vorangegangenen Resultate erfolgt. Mit diesem Vorgehen wird einerseits eine differenzierte Messung der Wirkung des IDG über einen längeren Zeitraum erfolgen, und andererseits wird eine aussagekräftige Berichterstattung des Datenschutzbeauftragten im jährlichen Tätigkeitsbericht gemäss § 39 IDG ermöglicht.

Schwerpunkte der Evaluation

Aufgrund eines Wirkungsmodells, welches die Bereiche Informationszugang und Datenschutz unterscheidet, hält das Konzept der ZHAW mögliche – beabsichtigte oder nicht beabsichtigte – Wirkungen des IDG fest. Darauf aufbauend werden diejenigen Aspekte konkretisiert, die in den folgenden Jahren im Detail evaluiert werden sollen. Mögliche Themen sind dabei die Sensibilisierung der Bevölkerung, die Erfüllung der Informationspflichten durch die öffentlichen Organe, die Respektierung des Gesetzmässigkeitsprinzips oder die Wirkung von Aufsichtsmassnahmen. Für jeden Bereich müssen in einem weiteren Schritt die konkreten Evaluationsfragen festgelegt werden und darauf basierend die jeweiligen Indikatoren. Nach der Durchführung dieser partiellen Evaluationen kann in einer weiteren Etappe eine Evaluationssynthese erstellt werden. Diese beruht auf den vorangegangenen spezifischen Evaluationen und kann noch weitere Elemente hinzufügen. Damit liegt nach einem Zeitraum von fünf bis sechs Jahren eine Gesamtevaluation des IDG vor, die als Grundlage für mögliche gesetzgeberische Massnahmen dienen kann.

Umsetzung der Evaluation

Das von der ZHAW vorgeschlagene etappenweise Vorgehen berücksichtigt die bestehenden personellen und finanziellen Ressourcen des Datenschutzbeauftragten, die keinen zusätzlichen Mitteleinsatz für die Berichterstattung über die Wirkung des IDG erlauben. Die Messungen der Wirkung basieren deshalb zu einem grossen Teil auf den vom Datenschutzbeauftragten im Rahmen des KEF erhobenen Indikatoren und den Feststellungen, die bereits heute in der Berichterstattung zum Tragen kommen. In einzelnen thematischen Bereichen wird es aber notwendig sein, dass zusätzliche Indikatoren erfasst werden, was mit zusätzlichem Aufwand verbunden sein wird.
Die kontinuierliche themenspezifische Evaluation erlaubt es damit, jährlich über einen bestimmten Bereich zu berichten, der Teil einer Gesamtevaluation sein kann, aber unter Umständen auch unmittelbaren Handlungsbedarf aufzeigt. Im nächsten Tätigkeitsbericht wird deshalb erstmals über einen thematischen Bereich berichtet werden.

Datenschutzbeauftragter

Nr. 9071
Funktionale Gliederung: 0

Finanzierung

Erfolgsrechnung (in Mio. Fr.)	R 11	B 12	Δ(P 13)	P 13	Δ(P 14)	P 14	Δ(P 15)	P 15	P 16	Δ%(11-16)
Ertrag	0.1	0.2	0.0	0.1	0.0	0.1	-0.0	0.1	0.1	
Aufwand	-2.0	-2.3	0.2	-2.3	0.2	-2.3	0.2	-2.3	-2.3	18.3
Saldo	-1.9	-2.1	0.2	-2.2	0.2	-2.2	0.2	-2.2	-2.2	
Investitionen (in Mio. Fr.)										Ø (11 -16)
Einnahmen										
Ausgaben			-0.1	-0.1						-0.0
Nettoinvestitionen			-0.1	-0.1						-0.0
Personal (Beschäftigungsumfang)	8.5	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	Direktions-ziel Nr.
E1	Begleitung und Überprüfung der Gesetzesanpassungen an die Vorgaben des IDG (Übergangsfrist)	2013	0
E2	Gesetzeskonformer Umgang mit Personendaten in sensitiven Bereichen fördern und fordern (Gesundheitswesen, Schule, Sozialbereich etc.)	2014	0
E3	Förderung der Umsetzung angemessener Massnahmen im Bereich der Informationssicherheit	2015	0

Indikatoren

Indikatoren	Art	R 11	B 12	P 13	P 14	P 15	P 16
Wirkungen							
W1 Anteil umgesetzter Hinweise bei Datenschutz-Reviews (%) (A3)	min.	35	60	60	60	60	60
W2 Anzahl Besuche auf Webseiten (A4)	min.	-	-	80'000	80'000	80'000	80'000
Leistungen							
L1 Anzahl Beratungen von Privatpersonen (A4)	max.	-	-	500	500	500	500
L2 Anzahl Vernehmlassungen und Mitberichte (A2)	P	-	-	18	18	18	18
L3 Anzahl Weiterbildungsangebote für öffentliche Organe (A2)	min.	-	-	15	15	15	15
L4 Anzahl Kontrollen (A3)	min.	-	-	30	30	30	30
Wirtschaftlichkeit							

Leistungsgruppe 9071	Budgetentwurf 2013
Budgetkredit Erfolgsrechnung (in Mio Fr.)	-2.173
Budgetkredit Investitionsrechnung (in Mio. Fr.)	-0.060
Leistungsindikatoren L1, L3 und L4	

Budget Leistungsgruppe 9071

Vom Budgetentwurf abweichende Budgetbeschlüsse des KR können hier eingeklebt werden

Anhang 1-10

Im Datenmeer untergehen?

«Big Data» ist das neue Schlagwort, das die unbegrenzte Auswertung riesiger Datenmengen beinhaltet.

Die Entwicklung ist schleichend. Im vergangenen Jahr hatte der Datenschutzbeauftragte zu beurteilen, ob es einem öffentlichen Organ erlaubt sein soll, gestützt auf die Daten, die ein Dritter bei sich selber bearbeitet, neue Erkenntnisse über seine eigenen Kundinnen und Kunden zu gewinnen (siehe Seite 25). Technisch läuft dies so ab, dass das öffentliche Organ bestimmte Personendaten an einen Dritten weitergibt. Dieser gleicht diese mit seiner eigenen Datensammlung ab, um weitere Informationen über die betroffenen Person zu finden. Im konkreten Fall lässt sich dies begrenzt und kontrolliert durchführen. Doch diese Art der Datenbearbeitung ist nur ein kleiner Hinweis darauf, was diesbezüglich auf uns zukommen wird.

Unbeschränkte Datenmengen

Immer häufiger werden riesige Datenmengen miteinander gekoppelt, denn in der Masse der Daten sollen neue Erkenntnisse gewonnen werden: Je grösser die Menge der Daten, desto höher wird die Chance für einen bahnbrechenden Informationsgewinn eingeschätzt. «Big Data» bezeichnet dabei die Ansammlung möglichst vieler Daten, die aus möglichst vielen Datenquellen zur Verfügung stehen. Da zunehmend alle Lebensbereiche digitalisiert werden, wird auch die Datenmenge weiterhin exponentiell wachsen.

Viele Auswertungen dieser Daten ermöglichen einen direkten oder indirekten Personenbezug. «Big Data» ist grundsätzlich eine Menge von anonymisierten Daten. Je grösser diese Menge ist, desto höher ist die Wahrscheinlichkeit, dass Daten einer bestimmten Person zugeordnet werden können. Studien zeigen auf, dass mit lediglich drei einfachen demografischen Merkmalen (Geschlecht, fünfstellige Postleitzahl und Geburtsdatum [Jahr, Monat, Tag]) zwischen 61 und 87 Prozent der US-Bevölkerung eindeutig identifizierbar werden: bei zirka 250 Millionen Menschen immerhin zwischen 150 und 220 Millionen Personen. Forscher haben auch nachgewiesen, dass anonyme Gensequenzen, die sich auf öffentlich zugänglichen Forschungsdatenbanken befinden, aufgrund der Kombination mit wenigen anderen Daten «deanonymisiert» werden können.

Datenschutz gewährleisten

Noch können diese Datenbearbeitungen im öffentlichen Bereich begrenzt werden. Doch je länger, je mehr wird «Big Data» auch Teil der Datenbearbeitungen der öffentlichen Organe. Am weitesten fortgeschritten ist dies heute im wissenschaftlichen Bereich. Die Konsequenzen, die «Big Data» für die Persönlichkeitsrechte haben wird, lassen sich langsam erahnen. Deshalb wird eine öffentliche Diskussion sich mit Fragen beschäftigen müssen wie dem Zugang zu solchen Daten, der Begrenzung der Auswertung der Daten, der Integrität oder der Löschung von Daten. Den Datenschutz im Datenmeer zu verlieren, ist keine Alternative für die Bürgerinnen und Bürger.

Webpräsenz, Medienarbeit und soziale Netzwerke

Im Zentrum der Informationstätigkeit des Datenschutzbeauftragten standen 2012 der kontinuierliche Ausbau der Webpräsenz, die Bearbeitung von zahlreichen Medienanfragen und die Lancierung eines Twitter-Accounts.

Die wichtigsten Informationen auf einen Blick

Internet www.datenschutz.ch
Twitter twitter.com/dsb_zh

Am 24. Januar 2012 war es endlich so weit: Der Datenschutzbeauftragte ging mit seinem komplett überarbeiteten Webauftritt online und ist seither bezüglich Design und Technologie ein Teil des kantonalen Webportals. Die klar strukturierte Navigation sowie das benutzerfreundliche Content-Management haben sich im ersten Betriebsjahr rundum bewährt – die User finden schnell zu den gesuchten Informationen und die inhaltlichen Updates lassen sich rasch und unkompliziert realisieren.

Reges Interesse der Medienschaffenden am Datenschutz

2012 verzeichnete der Datenschutzbeauftragte wiederum eine grosse Anzahl Anfragen von Journalistinnen und Journalisten aus der ganzen Schweiz. Im Zentrum des Interesses standen dabei die Risiken von sozialen Netzwerken und mobilen Geräten wie Smartphones und Tablets, die Transparenz bei Lohn- und Finanzinformationen und der Schutz von Gesundheitsdaten. Zu den Themen Ortungstechnologien und Internetpranger gab der Datenschutzbeauftragte ebenfalls mehrmals Auskunft.

Das anlässlich des 6. Europäischen Datenschutztages am 28. Januar 2012 durchgeführte Mediengespräch stand ganz im Zeichen der internationalen Entwicklungen; insbesondere des Entwurfs

einer neuen EU-Rahmengesetzgebung, die neben einer generellen vorgängigen Einwilligung der Betroffenen bei Datenpublikationen, dem so genannten Opt-in, auch griffige Interventionsrechte der Datenschutzbeauftragten und ein «Recht auf Vergessen» durch das sofortige Löschen von Daten auf Verlangen vorschlägt.

Das beherrschende Thema der Jahresmedienkonferenz vom 27. Juni 2012 war die Kontrolltätigkeit des Datenschutzbeauftragten, mit denen die Datenbearbeitungen einzelner öffentlicher Organe überprüft werden. Dabei wurde die Wichtigkeit unterstrichen, Leitlinien für die Informationssicherheit und Sicherheitskonzepte zu erarbeiten sowie in die Sensibilisierung und Schulung der mit Datenbearbeitungen betrauten Mitarbeitenden zu investieren.

Hilfestellungen für den modernen Arbeitsalltag

Die zahlreichen Geschäfte und Anfragen zu den Risiken von sozialen Netzwerken und mobilen Geräten veranlassten den Datenschutzbeauftragten 2012, mehrere Checklisten, Merkblätter und Leitfäden zu den Themen Nutzung von Cloud Computing, Einsatz von Smartphones und Tablet PCs, Sicherheit von Smartphones sowie Privacy-Einstellungen bei Facebook und Internetbrowsern zu veröffentlichen. Diese zeigen den öffentlichen Organen und Benützenden auf, welche Punkte bei Nutzung und Einsatz dieser modernen Technologien und Geräte beachtet werden müssen, damit die Risiken für eine Verletzung der Privatsphäre möglichst gering bleiben. Alle Publikationen können auf www.datenschutz.ch unter der Rubrik «Veröffentlichungen» heruntergeladen werden.

#Datenschutz, #Privacy, #Informationssicherheit, #Security

Seit dem 8. November 2012 ist der Datenschutzbeauftragte mit einem eigenen Twitter-Account in den Sozialen Medien präsent, und kann unter dem Link http://twitter.com/dsb_zh erreicht werden.
Über Twitter wurden seitdem eigene News publiziert, aber auch auf Inhalte von Experten und Partnerinstitutionen aus der Datenschutz-Community hingewiesen. Die Themen #Datenschutz, #Privacy, #Informationssicherheit und #Security standen im Zentrum der durchschnittlich zwei wöchentlichen Tweets.
Im Zusammenhang mit dem Twitter-Auftritt hat der Datenschutzbeauftragte einen Disclaimer erarbeitet, der die wichtigsten Richtlinien, Hinweise und Vorkehrungen zur sicheren Nutzung dieses Kommunikationskanals beinhaltet und der auch erklärt, weshalb er sich für eine Präsenz auf Twitter entschieden hat und wie er sich im Social-Media-Umfeld zu bewegen gedenkt.

Sensibilisierung durch Weiterbildung

2012 fanden verschiedene Weiterbildungskurse für Mitarbeitende von öffentlichen Organen statt. Mit Referaten, Präsentationen und Anlässen zum Thema Datenschutz und Informationssicherheit wurden Entscheidungsträger und Stakeholder sensibilisiert.

Ausgewählte Präsentationen und Referate 2012

- Herausforderungen des Datenschutzes im internationalen Kontext
- Cloud Computing
- Privacy im Internet
- Privacy in sozialen Netzwerken
- Smartphone-Sicherheit
- Sensibilisierung Informationssicherheit
- Datenschutz und Öffentlichkeitsprinzip in der Beruflichen Vorsorge sowie Stiftungsaufsicht
- Datenschutz in der Schule

Das Anbieten von Aus- und Weiterbildungen gehört zu den Aufgaben des Datenschutzbeauftragten. Mit über die Website allgemein zugänglichen Lernprogrammen werden den Mitarbeitenden von öffentlichen Organen und interessierten Dritten die Grundlagen des Datenschutzes und der Informationssicherheit vermittelt.

Seminar-Konzept hat sich bewährt

Das im Vorjahr überarbeitete Konzept für Seminare konnte 2012 in wesentlichen Punkten umgesetzt werden: Die Ausbildungsinhalte wurden aktualisiert und in zielgruppenspezifischen Modulen zusammengefasst. Ziel war es, ein Grundangebot für Juristinnen und Juristen sowie Fachleute aus den Gemeinden, aber auch für Informatikverantwortliche zur Verfügung zu stellen. In sensiblen datenschutzrechtlichen Bereichen wie dem Sozial- oder Gesundheitswesen werden spezifische Vertiefungsseminare angeboten.

Praxisorientierte Weiterbildung für Fachleute

Am 20. November 2012 organisierte der Datenschutzbeauftragte wiederum eine fachspezifische Weiterbildung für Angestellte im Gesundheitswesen, die mit der Bearbeitung besonders sensibler Personendaten betraut sind. Bei der Schulung standen die Klärung und die Beantwortung recht-

licher, organisatorischer und technischer Fragestellungen der Mitarbeiterinnen und Mitarbeiter im Umgang mit Personendaten im Zentrum. Den Mitarbeitenden wurden dabei die Grundsätze des Datenschutzes und der Informationssicherheit sowie die spezifischen Problemstellungen und Geheimhaltungsbestimmungen vermittelt. Es wurden auch aktuelle Trends und Entwicklungen diskutiert sowie Fälle aus der Praxis bearbeitet. Der Kurs wurde 2012 zum wiederholten Mal angeboten und findet einmal jährlich statt.

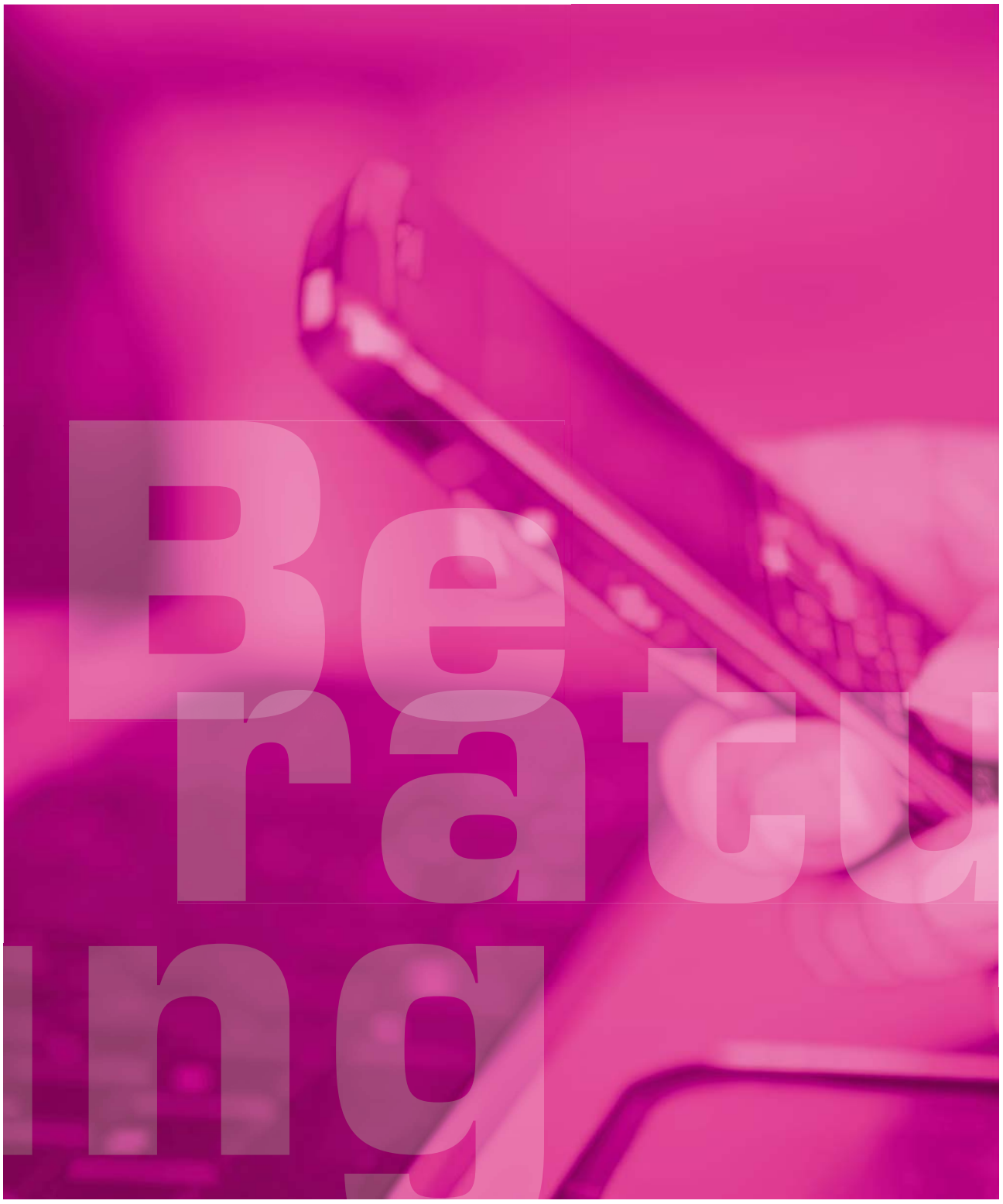
Tradition hat auch das in Zusammenarbeit mit der Koordinationsstelle IDG der Staatskanzlei organisierte Seminar zum Öffentlichkeitsprinzip, das am 19. Juni 2012 durchgeführt wurde. Die Weiterbildung richtet sich primär an Verwaltungsmitarbeitende ohne juristische Ausbildung und bietet praktische Hilfestellungen im Umgang mit den verschiedenen Verwaltungsinformationen. Die Vermittlung des korrekten Vorgehens bei Informationen von Amtes wegen sowie bei der Behandlung von Zugangsgesuchen zu Verwaltungsdokumenten stehen dabei im Zentrum der Schulung.

Symposium «Wo sind die Daten?»

Bereits zum 17. Mal fand Ende August 2012 das vom Datenschutzbeauftragten mitorganisierte Symposium on Privacy and Security statt. Ziel ist es, die Öffentlichkeit auf die Bedeutung von Privatheit und Sicherheit in der Informations- und Wissensgesellschaft aufmerksam zu machen sowie Bestrebungen zur Verbesserung des Datenschutzes und der Informationssicherheit zu unterstützen. 2012 war die Veranstaltung dem Thema «Ausgelagerte Datenbearbeitungen» gewidmet. Dabei wurde aufgezeigt, wie die rechtlichen, organisatorischen und technischen Massnahmen ausgestaltet sein müssen, damit Vertrauen in die Datenbearbeitung durch Dritte geschaffen werden kann.

Massgeschneiderte Präsentationen

Auf Anfrage bietet der Datenschutzbeauftragte auch Kurse und Seminare für einzelne öffentliche Organe oder Betriebe an oder hält Referate zum Thema Datenschutz und Informationssicherheit in Lehrgängen. Eine Übersicht ausgewählter Referate aus dem Berichtsjahr findet sich auf Seite 17.



«Der Einsatz neuer Technologien ist Anlass für viele Beratungen.»

Cloud Computing, Facebook & Co in der Beratungstätigkeit

Die Gestaltung und der Einsatz datenschutzfreundlicher Technologien sowie deren Nutzung stellen eine grosse Herausforderung dar. Sowohl die öffentlichen Organe als auch Privatpersonen, welche ihre Rechte geltend machen, werden mit diesen Themen konfrontiert. Mit Beratungen, Merkblättern und Checklisten unterstützt der Datenschutzbeauftragte Verantwortliche und Betroffene.

Beratung

Anfragen zu den Voraussetzungen bei einem Outsourcing, insbesondere unter Inanspruchnahme von Informatikleistungen, allenfalls mit Nutzung von Cloud-Diensten, standen ebenso auf der Tagesordnung wie Anfragen zu angemessenen Sicherheitsmassnahmen etwa bei der Inanspruchnahme mobiler Geräte am Arbeitsplatz. Die Bürgerinnen und Bürger hatten auch Fragen zum Umgang der Verwaltung mit ihren Daten und zu ihren Datenschutzrechten.

Die Themen der vom Datenschutzbeauftragten durchgeführten Beratungen waren 2012 erneut breit gefächert. Schwerpunkte waren wie bereits in den Vorjahren der Einsatz relativ neuer Technologien wie Cloud Computing, die Verwendung mobiler Geräte am Arbeitsplatz, Publikationen im Internet oder die Nutzung von Daten Dritter zur Durchführung von Bonitätsprüfungen.

Cloud Computing

Allein aufgrund der aus wirtschaftlicher Sicht beachtlichen Vorteile bei der Nutzung von Cloud Computing dürfen die datenschutzrechtlichen Rahmenbedingungen nicht vergessen werden. Wer hat die Kontrolle? Wo gehen die Daten hin? Wer hat Zugriff? Können die Informationen unwiderruflich gelöscht werden? Diese und weitere Fragen stellen sich jedem Nutzer einer Cloud. Die Antworten finden sich im Merkblatt der Datenschutzbeauftragten zum Thema Cloud Computing sowie in den ebenfalls publizierten Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen. Beide Publikationen wurden 2012 fertig gestellt und können auf der Website des

Datenschutzbeauftragten (www.datenschutz.ch) heruntergeladen werden.

Publikationen im Internet

Publikationen im Internet bergen höhere Gefahren für die Persönlichkeitsrechte Betroffener als herkömmliche Veröffentlichungen. Deshalb ist neben der Auslegung der Fachgesetze und der Rahmenbedingungen des IDG immer auch die Verhältnismässigkeit zu beachten. Eine beschränkte Publikationsdauer etwa oder Mechanismen zur Verhinderung der Indexierung durch Suchmaschinen können hier Abhilfe schaffen. Dazu gehört auch, dass bei Informationen, welche durch das öffentliche Organ ins Netz gestellt werden und über das Allgemeine hinausgehen, wie beispielsweise bei der Veröffentlichung von Fotos, die vorgängige Einwilligung der Betroffenen eingeholt wird. Im Berichtsjahr hat der Datenschutzbeauftragte mehrere Webartikel dazu veröffentlicht – diese können unter www.datenschutz.ch, Rubrik «Themen, Publikation im Internet» eingesehen werden.

Soziale Medien

Viele Leute können sich ein Leben ohne das Nutzen sozialer Netzwerke nicht mehr vorstellen. Letztere ermöglichen eine äusserst schnelle Vernetzung, bergen aber auch das Risiko, dass ungewollt und aus Versehen persönliche Informationen der Allgemeinheit zugänglich gemacht werden. Die richtigen Datenschutzeinstellungen, um sich vor ungewolltem Zugriff und gar Missbrauch zu schützen, finden sich in den Checklisten «Privacy Facebook», «Smartphone-Sicherheit», «Privacy Internet Explorer» sowie «Privacy Firefox», die auf der Website des Datenschutzbeauftragten www.datenschutz.ch unter der Rubrik «Veröffentlichungen» publiziert sind.

01
Gemeinderatssitzungen sind nicht öffentlich

Eine Gemeinde gelangte mit der Frage an den Datenschutzbeauftragten, ob eine Möglichkeit bestehe, im Sinne des Öffentlichkeitsprinzips und des Wunsches nach mehr Transparenz in der Verwaltung öffentliche Sitzungen des Gemeinderats (Exekutive) durchzuführen. Die Gemeinde verwies dabei auf den Kanton Solothurn, welcher seine Regierungs- bzw. Gemeinderatssitzungen öffentlich durchführt.
Im Kanton Zürich umfasst das Öffentlichkeitsprinzip den freien Zugang zu amtlichen Dokumenten und das Recht jeder Person auf Einsichtnahme in Behördenakten, solange keine Geheimhaltungspflicht für ein bestimmtes Dokument besteht. Vom Öffentlichkeitsprinzip ausgenommen bleibt jedoch das gesetzlich verankerte Sitzungsgeheimnis. Das Öffentlichkeits- und Transparenzprinzip ist aber gleichwohl gewährleistet, indem Beschlüsse der Gemeindeexekutiven veröffentlicht werden, sofern keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen.
Der Datenschutzbeauftragte verwies die Gemeinde auf den klaren Wortlaut des Gemeindegesetzes, welches die Öffentlichkeit explizit von den Gemeinderatssitzungen ausschliesst. Die unmittelbare Öffentlichkeit von Gemeinderatssitzungen bedürfte somit einer Revision des geltenden Rechts.
Aus datenschutzrechtlicher Sicht müsste eine Bestimmung, welche die Öffentlichkeit von Sitzungen der Gemeindeexekutive vorsieht, auch Mechanismen enthalten, um die Persönlichkeitsrechte der Betroffenen sicherzustellen, wie dies im Kanton Solothurn der Fall ist.

§§ 14, 20 Abs. 1 und 23 IDG
§§ 69 und 68a GG

02
Rahmenbedingungen zur Veröffentlichung des Amtsblatts im Internet

Eine Gemeinde publizierte das Amtsblatt auf ihrer Website. Aufgeschaltet wurden neben Wahl- und Abstimmungsresultaten sowie Mitteilungen allgemeiner Natur auch Baubewilligungen und Baugesuche mit den entsprechenden Personendaten. Dabei waren alle Ausgaben seit 2008 online verfügbar und die darin enthaltenen Informationen über Suchmaschinen auffindbar. Der Datenschutzbeauftragte hat sich im Folgenden zur Publikationsdauer geäussert und auch dazu, wie das Auffinden durch Suchmaschinen verhindert werden kann.
Im vorliegenden Fall handelte es sich bei den im Internet publizierten Daten überwiegend um Sachdaten und gewöhnliche Personendaten. Soweit eine gesetzliche Bestimmung nicht ausdrücklich eine Bekanntmachung in elektronischer Form erlaubt, ist durch Auslegung der entsprechenden Bestimmung zu ermitteln, ob die darin enthaltene Ermächtigung zur Veröffentlichung auch eine Bekanntmachung dieser Information im Internet umfasst. Weiter muss die Publikation verhältnismässig sein, was die publizierten Daten und die Dauer der Veröffentlichung betrifft. Personendaten, an denen kein öffentliches

Interesse mehr besteht, sind aus dem Internet zu entfernen. So wird beispielsweise in den Publikationsverordnungen von Kanton und Stadt Zürich die Publikationsdauer auf drei Monate beschränkt. Zusätzlich wies der Datenschutzbeauftragte auf die Möglichkeit hin, dass durch das Setzen von entsprechenden Definitionen auf der Website die Indexierung und Archivierung bei Suchmaschinen verhindert werden kann.
Die Gemeinde veröffentlicht fortan nur noch die letzten vier Ausgaben ihres Amtsblatts im Internet.

§§ 8 Abs. 1 und 14 IDG

03
Online-Zugriff der KESB auf Einwohnerregister klar geregelt

Eine Gemeinde wandte sich an den Datenschutzbeauftragten, da die Kindes- und Erwachsenenschutzbehörde (KESB) einen Online-Zugriff auf das Einwohnerregister gewünscht hatte. Die KESB verlangte den Zugriff auf Namen, Vornamen, Geburtsdatum, Zivilstand, Adresse, Heimatort, Beruf, Zuzugs- und Wegzugsort, Zuzugs- und Wegzugsdatum, Angaben über Familienverhältnisse, Haus- und Wohngemeinschafts- sowie weitere Angaben.
Rechtsgrundlage für einen Online-Zugriff der KESB auf die Einwohnerregister ist das neue Einführungsgesetz zum Kindes- und Erwachsenenschutzrecht (EG KESR), das auf den 1. Januar 2013 in Kraft getreten ist. Nach dieser Bestimmung können die KESB in hängigen Verfahren Zugriff auf Name, Vorname, Geburtsdatum, Heimatort, Geschlecht, Zivilstand, Adresse, Beruf, Datum und Herkunftsort bei Zuzug sowie Datum und Zielort bei Wegzug erhalten.
Die Direktion der Justiz und des Innern und der Datenschutzbeauftragte, die gleichzeitig angefragt wurden, hielten übereinstimmend fest, dass der im Gesetz angeführte Katalog der Daten, auf die zugegriffen werden darf, abschliessend ist. Die KESB hat somit standardmässig Zugriff auf diese Daten, sofern die Gemeinde diesen ermöglicht; eine Verpflichtung, den Zugriff tatsächlich zu gewähren, besteht hingegen nicht. Da im Voraus nicht bestimmt werden kann, welche Personen in ein Verfahren vor einer KESB involviert sein werden, muss ein Zugriffsrecht auf die entsprechenden Daten aller Einwohnerinnen und Einwohner der jeweiligen Gemeinde bestehen. Zweck des Zugriffs ist die Abklärung der örtlichen Zuständigkeit der KESB, wenn ein Verfahren anhängig gemacht wird, sowie die Identifikation der betroffenen Person; entsprechend diesem Zweck können Zugriffsrechte nur der örtlich zuständigen KESB erteilt werden. Die KESB darf vom Zugriffsrecht selbstverständlich nur Gebrauch machen, wenn bei ihr ein Fall anhängig gemacht wird. Benötigt sie im Einzelfall weitere Daten, sind diese in erster Linie bei der betroffenen Person zu beschaffen. Subsidiär sind auch einzelfallweise Anfragen bei den Einwohnerkontrollen möglich.
Zum Zeitpunkt der Anfrage war eine Verordnung zu § 74 EG KESR in Ausarbeitung, welche die Bestimmung insbesondere in Bezug auf die Erteilung der Zugriffsrechte und die Protokollierung der Zugriffe konkretisieren soll (siehe dazu auch Seite 33).

§ 74 EG KESR

04
Keine polizeilichen Abklärungen bei Einbürgerungen durch die Gemeinde

Eine Gemeinde sah sich mit einem Einbürgerungsgesuch konfrontiert, bei dem sich aus den Gesuchsakten keine Hinweise auf ein strafrechtliches Verhalten ergaben. Das Gespräch mit der gesuchstellenden Person wies hingegen auf eine strafrechtlich relevante Vergangenheit hin. Die Gemeinde gelangte mit der Frage an den Datenschutzbeauftragten, inwieweit weitere Abklärungen beispielsweise in Bezug auf Einträge in polizeilichen Datenbanken möglich seien.
Für die Bearbeitung von besonderen Personendaten bedarf es einer hinreichend bestimmten Regelung in einem formellen Gesetz. Bei der ordentlichen Einbürgerung von ausländischen Staatsangehörigen beurteilt die Direktion der Justiz und des Innern, ob die gesuchstellende Person die Wohnsitzerfordernisse des Bundes erfüllt und sich zur Einbürgerung eignet. Dazu gehört namentlich auch die Prüfung, ob eine gesuchstellende Person die schweizerische Rechtsordnung beachtet und ob sie die innere sowie äussere Sicherheit der Schweiz nicht gefährdet. Die Gemeinde darf somit keine selbständigen polizeilichen Abklärungen tätigen. Sie darf von der gesuchstellenden Person auch nicht verlangen, einen Auszug aus dem polizeilichen Informationssystem Polis einzuholen.
Ergeben sich aus der Befragung durch die Gemeinde aber Anhaltspunkte, dass sich eine gesuchstellende Person nicht an die schweizerische Rechtsordnung hält, kann der Gemeinderat bei der Direktion der Justiz und des Innern beantragen, diesbezüglich weitergehende Abklärungen vorzunehmen. Im Auftrag der Direktion der Justiz und des Innern sowie mit Zustimmung der Gemeinde können diese auch durch die Gemeindepolizei durchgeführt werden.

§ 8 Abs. 2 IDG
§ 21 Abs. 2 lict. c und d BüV
§ 26 Abs. 1 und 2 BüV

05
Abruf von Handelsregisterbelegen über das Internet

Das Handelsregisteramt erweiterte per 1. Juli 2012 seine Online-Dienstleistungen. Belege, welche den Einträgen im Handelsregister zugrunde liegen, sind nicht mehr nur am Schalter einsehbar, sondern können auch über das Internet abgerufen werden. Klickt man auf das Symbol für einen Beleg, wird man dazu aufgefordert, Name und E-Mail-Adresse einzugeben. Anschliessend werden die Dokumente unverzüglich und kostenlos elektronisch zugestellt. E-Mail-Adresse, Name und Dateiname des Dokuments werden in einer Datenbank des Handelsregisteramts gespeichert.
Verschiedene Privatpersonen gelangten im Herbst 2012 mit der Frage an den Datenschutzbeauftragten, ob die Veröffentlichung der Belege zulässig sei. Problematisch ist dies insbesondere dann, wenn Belege sensible Informationen über Personen enthalten (beispielsweise Stiftungsratsprotokolle von BVG-Einrichtungen mit Daten über IV-Bezüger). Die Abklärungen des Datenschutzbeauftragten haben ergeben, dass der Abruf von Belegen über das Internet zulässig ist. Ein öffentliches Organ darf Personendaten bekannt geben, wenn eine rechtliche Bestimmung dazu ermächtigt und der Grundsatz der Verhältnismässigkeit gewahrt wird. Das Handelsregister mit Ein-

schluss der Anmeldungen und der Belege ist gemäss spezialgesetzlichen Vorschriften öffentlich. Der elektronische Zugriff auf die Belege wird von den bestehenden Rechtsgrundlagen somit gedeckt. Die Belege sind nicht direkt im Internet einsehbar, sondern werden den Interessierten per E-Mail zugestellt. Das Handelsregisteramt registriert Name und E-Mail-Adresse der abfragenden Personen sowie den Dateinamen des ausgelieferten Dokuments. Zudem lässt es das geltende Recht zu, dass dem Handelsregister lediglich Protokollauszüge statt ganze Protokolle eingereicht werden. Aufgrund dieser Umstände bejahte der Datenschutzbeauftragte die Verhältnismässigkeit. Insgesamt stellt der Abruf von Belegen über das Internet lediglich eine Anpassung der Dienstleistungen des Handelsregisteramts an den heutigen Stand der Technik dar.

Damit jedoch keine Informationen über Personen bekannt gegeben werden, welche nicht handelsregisterrelevant sind, sind die betroffenen Unternehmen dahingehend zu sensibilisieren, dass sie dem Handelsregisteramt nur jene Belege einreichen, die tatsächlich erforderlich sind.

§ 16 Abs. 1 lit. a IDG
Art. 930 OR
Art. 10 und 23 HRegV

06
Bonitätsprüfungen durch öffentliche Organe bedingen klare Rahmenbedingungen

Ein öffentliches Organ möchte automatisierte Bonitätsprüfungen über neue Kunden durchführen und unterbreitete dieses Projekt dem Datenschutzbeauftragten zur Beurteilung. Es soll mit einem externen Partner zusammengearbeitet werden, der die Daten des öffentlichen Organs mit seinen eigenen über die Kunden verfügbaren Informationen abgleichen und Personen mit schlechter Bonität an das öffentliche Organ zurückmelden.
Dieser Sachverhalt tangiert gleich zwei datenschutzrechtlich relevante Aspekte: Das Outsourcing und das Scoring. Was das Outsourcing betrifft, so bleibt das öffentliche Organ auch für die durch den Dritten durchgeführte Datenbearbeitung verantwortlich. Der externe Partner darf folglich die Informationen nur so bearbeiten, wie es das öffentliche Organ selbst darf. Es dürfen nur diejenigen Daten übermittelt werden, welche zur Abklärung der Bonität geeignet und erforderlich sind. Der externe Partner darf die Informationen auf keinen Fall für die Erweiterung der eigenen Datensammlung benützen oder zu anderen als den genannten Zwecken bearbeiten. Die im IDG stipulierten Voraussetzungen für eine Datenbearbeitung durch Dritte, nämlich dass keine rechtliche Bestimmung oder vertragliche Vereinbarung diesem Outsourcing entgegen steht, muss eingehalten werden; insbesondere muss ein schriftlicher Vertrag vorliegen, dessen Inhalt dem Schutzbedürfnis der Daten angepasst ist.
Bei Bonitätsprüfungen, welche automatisiert ausgeführt werden – dem so genannten Scoring – besteht die Gefahr, dass ungesicherte und/oder unkorrekte Aussagen über Personen erfasst und bearbeitet werden. Die Richtigkeit dieser Daten kann durch die betroffenen Personen kaum überprüft werden, so dass zusätzliche Schutzmassnahmen umzusetzen sind. Der Kunde ist auf dieses Scoring hinzuweisen und bei einer Negativmeldung über die Herkunft des Resultats zu orientieren. Es ist sicherzustellen, dass Betroffene ihre berechtigten Interessen respektive ihren Standpunkt geltend machen können. Dazu können auch Korrekturansprüche bei einer unzulässigen oder falschen Datenbasis oder einer nicht korrekten Berechnung gehören.

§ 6 IDG
§ 25 IDV

07
Videoüberwachung in einem öffentlichen Spital muss verhältnismässig sein

Ein öffentliches Spital plante die stufenweise Einführung von Videoüberwachung, um die zahlreichen Gebäude und Eingänge besser kontrollieren zu können. In einem ersten Schritt sollten die Zugänge bestimmter Bereiche mit einem Türschliesssystem ausgerüstet werden, wobei Netzwerkkameras zum Einsatz kommen sollten. Im Vordergrund stand die Überwachung der Eingänge zur Klinik für Neonatologie, um Entführungen von Neugeborenen sowie familiäre Gewalt im Spitalraum zu verhindern. Das Spital bat den Datenschutzbeauftragten um eine datenschutzrechtliche Beurteilung des Projekts.
Der geplante Einsatz von Netzwerkkameras bei Türschliesssystemen war als Echtzeit-Videoüberwachung zu qualifizieren, da lediglich eine Live-Schaltung der Aufnahmen zur Prüfung beabsichtigt war, um festzustellen, wer vor der Tür steht. Videoüberwachungen bedürfen einer gesetzlichen Grundlage und müssen verhältnismässig sein. Informationen über die Gesundheit gelten als besondere Personendaten und dürfen nur bearbeitet werden, wenn eine hinreichend bestimmte Grundlage in einem formellen Gesetz dies erlaubt. Die Tatsache, dass jemand ein Spital betritt, lässt gewisse Rückschlüsse auf seine Gesundheit oder auf die seiner Angehörigen zu. Werden die Aufnahmen jedoch nur an die Personen übermittelt, welche für die Türkontrolle zuständig sind, und werden keine besonderen technischen Mittel eingesetzt, welche die Persönlichkeit der abgebildeten Personen stärker beeinträchtigen als die Betrachtung von blossem Auge, kann dies mit einer physischen Präsenz von Mitarbeitenden an der Eingangstür gleichgesetzt werden. Auf diese Weise eingesetzte Kameras dienen der Erfüllung gesetzlich umschriebener Aufgaben des Spitals und dürfen ohne eine spezifisch auf die Videoüberwachung gerichtete gesetzliche Grundlage betrieben werden. Kameras dürfen allerdings nur eingesetzt werden, wenn sie zur Erreichung des Zwecks geeignet und erforderlich sind. Insbesondere dürfen keine milderen, weniger stark in die Persönlichkeit eingreifenden Massnahmen zur Verfügung stehen wie beispielsweise Massnahmen personeller oder baulicher Art.
Die Beurteilung der Verhältnismässigkeit obliegt in erster Linie dem Spital, welches die örtlichen Gegebenheiten und die spezifischen Risiken kennt. Erachtet das Spital den Einsatz von Kameras als erforderlich, so hat es vorgängig ein entsprechendes Reglement zu erlassen. Darin sind der Schutzzweck des Kameraeinsatzes, die zulässige Nutzung und die Verantwortlichkeiten festzulegen. Aus Transparenzgründen ist das Reglement für die interessierte Öffentlichkeit zugänglich zu halten.

§ 8 Abs. 1 IDG

08
Massnahmen zur sicheren Auslagerung eines elektronischen Archivs

Ein Spital plante, sein elektronisches Archiv auszulagern. Der Datenschutzbeauftragte prüfte, ob aus datenschutzrechtlicher Sicht Vorbehalte gegen ein solches Outsourcing bestehen.
Das betroffene Spital ist eine Anstalt des kantonalen öffentlichen Rechts mit eigener Rechtspersönlichkeit und gilt als öffentliches Organ im Sinne des IDG. Damit kommen die Rahmenbedingungen der Auftragsdatenbearbeitung zum Tragen. Massgebend ist, dass dieser Auslagerung keine rechtlichen Bestimmungen entgegenstehen und der Inhalt des abzuschliessenden Vertrages dem Schutzbedürfnis der Daten angemessen Rechnung trägt.
Das Spital bleibt auch nach der Auslagerung für die Datenbearbeitung verantwortlich.
Informationen, die durch das Spital bearbeitet werden, sind besondere Personendaten und sowohl durch das Amts- als auch durch das Berufsgeheimnis geschützt. Das Amtsgeheimnis steht der Auslagerung nicht entgegen. Mit dem Abschluss des Outsourcingvertrags wird der Auftragnehmer zur Hilfsperson des Spitals und ist dadurch auch an das Amtsgeheimnis gebunden. Ob dem Auftragnehmer auch die Geheimnispflichten im Sinne des Berufsgeheimnisses auf diese Weise übertragen werden können, ist in der Lehre umstritten. Um der Geheimnispflicht zu genügen, sind deshalb diejenigen Mitarbeitenden, welche die Daten bearbeiten, dem Weisungsrecht des Spitals zu unterstellen. Sie sind schriftlich zur Einhaltung der Schweigepflicht zu verpflichten. Ungeachtet der vertraglichen Regelungen müssen die Daten mit angemessenen organisatorischen und technischen Massnahmen geschützt werden. Dazu gehört beispielsweise, dass besondere Personendaten zu verschlüsseln sind, wobei das Spital für das Schlüsselmanagement verantwortlich bleibt. Eine weitere Massnahme besteht darin, den Zugriff auf möglichst wenige Mitarbeitende zu beschränken.

§ 6 IDG
§ 25 IDV
§ 7 IDG

09
Umgang mit Lohnpfändungsanzeigen präzisiert

Das Personalamt erledigt für die kantonale Verwaltung zentral die Lohnadministration. Es erhält von Betreibungsämtern immer wieder direkt Lohnpfändungsanzeigen, vollzieht diese selbständig und erfasst die Lohnpfändung im Personal- und Lohnadministrationssystem (PULS). Eine Direktion intervenierte beim Personalamt, weil ein von einer Lohnpfändung betroffener Mitarbeiter in eine Leitungsfunktion hätte befördert werden sollen und die Vorgesetzten von der Lohnpfändung keine Kenntnis hatten. Das Personalamt verlangte eine datenschutzrechtliche Beurteilung, inwieweit die Anstellungsbehörden über eine Lohnpfändung informiert werden dürfen oder müssen.

Das Schuldbetreibungs- und Konkursgesetz (SchKG) bestimmt, dass bei der Pfändung von Forderungen (also auch Lohnforderungen) dem Schuldner des Betriebenen (also in diesem Fall dem Arbeitgeber) angezeigt wird, dass er rechtsgültig nur noch an das Betreibungsamt Zahlungen leisten könne. Den Lohn schuldet die Körperschaft «Kanton Zürich»; für die Durchführung des Arbeitsverhältnisses zuständig ist die jeweilige Anstellungsbehörde. Diese entscheidet, ob tatsächlich Lohn geschuldet ist und in welcher Höhe. Die Abteilung Payroll (früher Lohnadministration) des Personalamtes handelt bezüglich Lohnauszahlung jeweils im Auftrag der Anstellungsbehörden.

Demzufolge müsste eine Lohnpfändungsanzeige korrekterweise bei der Anstellungsbehörde eingehen.
Geht die Lohnpfändungsanzeige direkt beim Personalamt ein, ist sie an die Personalabteilung der Anstellungsbehörde weiterzuleiten. Diese hat den Vollzug der Lohnpfändung bei der Abteilung Payroll in Auftrag zu geben. Aus Praktikabilitätsüberlegungen werden bei der Abteilung Payroll eingehende Lohnpfändungsanzeigen direkt vollzogen und die Anstellungsbehörde erhält eine Information darüber.
Bei der Anstellungsbehörde ist auch zu entscheiden, welche weiteren Personen (beispielsweise direkte Vorgesetzte, Abteilungsleitende und/oder Amtsvorstehende) über die Lohnpfändung informiert werden. Dies hängt etwa davon ab, welche Funktion und welche Finanzkompetenzen der betroffene Mitarbeitende hat, ob in der gleichen Abteilung eine Häufung von Lohnpfändungen von Mitarbeitenden auftritt oder ähnlichen Überlegungen. Aufgrund der Beurteilung des Datenschutzbeauftragten hat das Personalamt eine entsprechende Vollzugsweisung zuhanden der Personaldienste der Direktionen und der Abteilung Payroll erlassen.

10
Gefährdungsmeldung durch Arbeitslosenkasse ist statthaft

Eine Arbeitslosenkasse wandte sich mit der Frage an den Datenschutzbeauftragten, ob sie betreffend einen Klienten eine Meldung an die Vormundschaftsbehörde machen dürfe. Der Klient sei psychisch auffällig, voller Hass auf alle Behörden und mit der Familie sowie der ganzen Welt unzufrieden. Drohungen habe er allerdings keine ausgesprochen. Die Arbeitslosenkasse war der Meinung, dass die Person psychische Hilfe benötige.
Die Arbeitslosenkassen sind Vollzugsorgane der Arbeitslosenversicherung; für sie gilt die Schweigepflicht gemäss dem allgemeinen Teil des Sozialversicherungsrechts (ATSG). Für eine Durchbrechung dieser Schweigepflicht braucht es eine gesetzliche Grundlage. Im Arbeitslosenversicherungsgesetz (AVIG) findet sich zwar ein Katalog von Tatbeständen, in denen Daten an andere Behörden weiter geleitet werden dürfen; eine Meldung an die Vormundschaftsbehörde ist jedoch nicht vorgesehen. Bis Ende 2012 war im Zivilgesetzbuch (ZGB) vorgesehen, dass Verwaltungsbehörden und Gerichte der Vormundschaftsbehörde Anzeige zu machen haben, sobald sie in ihrer Amtstätigkeit vom Eintritt eines Bevormundungsfalles wegen Geisteskrankheit oder Geistesschwäche Kenntnis erhalten haben. Ein solcher Fall war jedoch aufgrund des geschilderten Sachverhalts nicht gegeben. Auch das Bundesamt für Justiz und das Staatssekretariat für Wirtschaft vertraten die Ansicht, dass diese Bestimmung für eine Meldung nicht ausreiche. Dazu müsste ein Melderecht im AVIG selbst vorgesehen sein.

Auf den 1. Januar 2013 wurde das neue Kindes- und Erwachsenenschutzrecht (bisher: Vormundschaftsrecht) in Kraft gesetzt. Dabei wurden auch die entsprechenden Bestimmungen im AVIG angepasst. Neu dürfen Vollzugsorgane der Arbeitslosenversicherung der Kindes- und Erwachsenenschutzbehörde (KESB, bisher: Vormundschaftsbehörde) im Einzelfall auf deren schriftliches Gesuch hin Daten bekannt geben. Diese Bestimmung reicht aber weiterhin nicht aus, um aktiv Meldung zu erstatten. Gleichzeitig wurden auch die Melderechte und -pflichten im ZGB neu formuliert.

Gemäss ZGB können alle Personen der Kindes- und Erwachsenenschutzbehörde Meldung erstatten, wenn eine Person hilfsbedürftig erscheint. Wer in amtlicher Tätigkeit von einer hilfsbedürftig erscheinenden Person erfährt, ist hingegen zu einer Meldung verpflichtet. Diese Bestimmungen ersetzen und erweitern die bisherigen Meldepflichten. Lediglich die zur Wahrung des Berufsgeheimnisses nach Strafgesetzbuch verpflichteten Personen (wie Anwälte, Ärzte und Geistliche) müssen sich vom Berufsgeheimnis entbinden lassen, bevor sie eine solche Meldung erstatten.

Mit der neuen Rechtslage ab 2013 ist eine Gefährdungsmeldung durch Vollzugsorgane der Arbeitslosenversicherung an die KESB also möglich.

Art. 33 ATSG
Art. 97a AVIG
Art. 369 Abs. 2 ZGB
Art. 443 Abs. 1 ZGB
Art. 443 Abs. 2 ZGB
Art. 321 StGB

11
Öffentliche Organe im Bereich Kinder- und Jugendbetreuung

Anlässlich einer Gesetzesrevision erkundigte sich das Amt für Jugend und Berufsberatung beim Datenschutzbeauftragten, welche Institutionen und Privatpersonen, die im Bereich der Kinder- und Jugendhilfe agieren, als kantonale öffentliche Organe gelten und somit unter die kantonale Datenschutzgesetzgebung fallen.
Als öffentliche Organe gelten Organisationen des öffentlichen und privaten Rechts, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind. Eine öffentliche Aufgabe ist ein Anliegen, für welches der Staat eine gesteigerte Verantwortung übernimmt. Zwar handelt es sich bei der Betreuung und Erziehung von Kindern und Jugendlichen primär um eine privatrechtliche Angelegenheit, den Staat trifft jedoch eine Förderungsverantwortung zum Schutz der Kinder und Jugendlichen sowie zu ihrer Integration in die Gesellschaft. Welche Aufgaben im Bereich der Kinder- und Jugendhilfe als öffentlich und welche als privat anzusehen sind, muss daher anhand der Gesetzgebung näher betrachtet werden.
Der Datenschutzbeauftragte überprüfte den Grad der staatlichen Verantwortlichkeit konkret in Bezug auf private Kinder- und Jugendheime, Tageseltern, Pflegeeltern, private Vermittlungsstellen sowie private Kinderkrippen und -horte. Massgebende Kriterien waren unter anderem das Ausmass der staatlichen Reglementierung (wie zum Beispiel das Vorschreiben einer Bewilligungspflicht) und die Höhe der staatlichen Unterstützungsbeiträge. Der Datenschutzbeauftragte kam zum Schluss, dass lediglich beitragsberechtigte Kinder- und Jugendheime mit privater Trägerschaft eine öffentliche Aufgabe erfüllen und somit als kantonale öffentliche Organe zu qualifizieren sind. Tageseltern, Pflegeeltern, private

Vermittlungsstellen sowie private Kinderkrippen und -horte erfüllen hingegen keine öffentlichen Aufgaben und sind deshalb nicht als kantonale öffentliche Organe zu betrachten. Auf diese Akteure ist folglich die Datenschutzgesetzgebung des Bundes und nicht diejenige des Kantons anwendbar. Sollen sie zu einer Weitergabe von Personendaten ermächtigt oder verpflichtet werden, muss dies explizit in einer gesetzlichen Regelung vorgesehen sein, da sie als privatrechtliche Institutionen keine Amtshilfe leisten können.
Krippen und Horte, die auf einer öffentlich-rechtlichen Trägerschaft beruhen, beispielsweise als Teil einer Primarschule, fallen ohne Weiteres in den Anwendungsbereich des IDG. Bieten Krippen und Horte mit privater Trägerschaft im Auftrag der Gemeinde bzw. der Schule staatlich (mit)finanzierte Plätze an, gelten die Datenbearbeitungen als Auftragsdatenbearbeitungen. In solchen Fällen sind die Gemeinden angehalten, mit diesen Einrichtungen schriftlich Verpflichtungen zum Schutz der Personendaten und der Datensicherheit zu vereinbaren.

§ 3 Abs. 1 lit. c IDG
§ 6 IDG i.V.m. § 25 IDV
§§ 16 und 17 Abs. 2 IDG
§ 6 IDG
§ 25 IDV

12
Mitwirkungspflichten von Schulpsychologen

Das am 1. Januar 2013 in Kraft getretene neue Kindes- und Erwachsenenschutzrecht statuiert eine Mitwirkungspflicht von am Verfahren beteiligten Personen, wenn es um die Abklärung eines Sachverhalts geht. Gewisse Berufskategorien wie beispielsweise Ärztinnen und Ärzte unterliegen dieser Pflicht nur, falls sie von der geheimnisberechtigten Person dazu ermächtigt oder durch die vorgesetzte Stelle vom Berufsgeheimnis entbunden werden. In der Folge stellt sich die Frage, ob diese Bestimmungen auch für Schulpsychologinnen und -psychologen gelten. Je nachdem müssen auch sie vorgängig entweder eine Einwilligung der Betroffenen oder eine Entbindung vom Berufs- und/oder vom Amtsgeheimnis einholen.

Mit dem 2012 in Kraft getretenen Bundesgesetz über die Psychologieberufe unterstehen neu auch Psychologinnen und Psychologen dem Berufsgeheimnis. Dies gilt auch für Schulpsychologinnen und -psychologen, denn auch diese haben einen nach dem Bundesgesetz über die Psychologieberufe anerkannten Ausbildungsabschluss in Psychologie erworben. Es ist jedoch umstritten, ob die Schulpsychologinnen und -psychologen wegen der Unterstellung unter das Berufsgeheimnis auch zur im Zivilgesetzbuch aufgeführten Berufsgruppe zählen, obwohl sie dort nicht namentlich aufgeführt sind. Denn dies hätte zur Folge, dass sie nicht vorbehaltlos zur Mitwirkung verpflichtet wären und sich vorgängig vom Berufs- und vom Amtsgeheimnis entbinden lassen müssten.

Infolge der unklaren Rechtslage empfiehlt der Datenschutzbeauftragte, sich als Schulpsychologin oder -psychologe bei einer Aufforderung der Kindes- und Erwachsenenschutzbehörde zur Mitwirkung in einem Verfahren vom Berufs- und vom Amtsgeheimnis entbinden zu lassen.

Art. 448 Abs. 1 und 2 ZGB
Art. 321 Abs. 1 StGB

13
AHV-Nummer für Gymnasialaufnahmeprüfung nicht notwendig

Eine Schule verlangte für die Anmeldung zur Gymnasialaufnahmeprüfung auf ihrer Online-Plattform die AHV-Versichertennummer der Kandidatinnen und Kandidaten. Eine betroffene Person wandte sich mit dem Anliegen an den Datenschutzbeauftragten, die Zulässigkeit dieser Datenbearbeitung zu überprüfen. Die Verwendung und Bekanntgabe der AHV-Versichertennummer regelt das Bundesgesetz über die Alters- und Hinterlassenenversicherung (AHVG). Es ermächtigt die Bildungsinstitutionen zur systematischen Verwendung der AHV-Versichertennummer bei der Erfüllung ihrer gesetzlichen Aufgabe. Auf kantonaler Ebene bestimmt die Bildungsdatenverordnung, welche Datenkategorien über Lehrpersonen, Schülerinnen und Schüler verwendet werden dürfen. Die AHV-Versichertennummer wird nur unter der Rubrik «Lehrpersonen» aufgeführt. Auch wenn das AHVG die Verwendung der AHV-Versichertennummer im Bildungswesen grundsätzlich erlaubt, sprach sich der Kanton gegen die Verwendung der AHV-Versichertennummer von Schülerinnen und Schülern im Bereich der Bildungsverwaltung aus. Eine bundesrechtliche Verpflichtung zur Bearbeitung der AHV-Versichertennummer besteht nur im Bereich der Bildungsstatistik.

Im beurteilten Fall wurden die Daten zu administrativen und nicht zu statistischen Zwecken erhoben. Nachdem der Datenschutzbeauftragte auf die beschriebene Rechtslage hingewiesen hatte, beschloss das Mittelschul- und Berufsbildungsamt, in Zukunft auf die Erhebung der AHV-Versichertennummer zu verzichten und das Anmeldeverfahren entsprechend anzupassen.

§ 8 Abs. 1 IDG
Art. 50e Abs. 2 lit. d AHVG
§ 1 und 4 Bildungsdatenverordnung
Art. 2 Abs. 1 lit. a BStatG i.V.m. mit Ziff. 69 Anhang zur Statistikerhebungsverordnung

14
Klare Bedingungen für Fotofallen im Wald

Die Jägerschaft im Kanton Zürich setzt vermehrt Kameras, so genannte «Fotofallen», zur Wildbeobachtung im Wald ein. Es handelt sich um Aufnahmegeräte, die an bestimmten Orten im Wald aufgestellt werden, beispielsweise bei einem Fuchs- oder Dachsbau oder einer Futterkrippe. Die Aufnahmen werden bei einer Bewegung im Aufnahmebereich automatisch ausgelöst. In der Praxis ist nicht ausgeschlossen, dass auch Menschen solche Aufnahmegeräte auslösen und damit in ihrer Privatsphäre tangiert sein können. Gemäss Zivilgesetzbuch ist es grundsätzlich jedermann gestattet, Waldgebiete zu betreten und sich darin aufzuhalten und zu bewegen. Das Amt für Landschaft und Natur (ALN) entwarf deshalb ein Merkblatt betreffend die Verwendung von Fotofallen zuhanden von Jagdgesellschaften, Wildhütern und anderen interessierten Zielgruppen und bat den Datenschutzbeauftragten um eine entsprechende Stellungnahme.
Die Aufgaben von Wildhütern und Jägerschaft bestehen unter anderem darin, Wildtierbestände zu erheben, Standorte bestimmter Wildarten festzustellen und zur Regulierung der Bestände einen effizienten Jagdbetrieb zu gewährleisten. Für die Erfüllung dieser gesetzlichen Aufgaben kann sich der Betrieb von Fotofal-

len rechtfertigen. Die datenschutzrechtlichen Voraussetzungen, welche dabei erfüllt sein müssen, hat das ALN im Merkblatt festgehalten: An öffentlichen Plätzen, entlang von Spazier- und Wanderwegen oder an viel begangenen Orten sind Fotofallen nicht zulässig. Die installierten Aufnahmegeräte und Standorte müssen signalisiert werden, und auf den Wildkameras muss die Kontaktadresse des Betreuers oder der Betreuerin vermerkt sein. Aufnahmen von Personen sind umgehend zu löschen und dürfen weder abgespeichert noch weitergegeben werden. Der Betreuer oder die Betreuerin der Wildkameras muss diese und die integrierten Speichermedien gegen Diebstahl und Vandalismus sichern.
Der Datenschutzbeauftragte begrüsste die Initiative des ALN und teilte diesem mit, dass die im Merkblatt angeführten Bedingungen für den Betrieb von Fotofallen den datenschutzrechtlichen Voraussetzungen entsprechen.

Art. 699 ZGB

15
Datenschutzkonformer Einsatz von Google Analytics nicht gewährleistet

Google Analytics ist eine Software, mit welcher das Besucherverhalten, das so genannte Besuchertracking, auf Websites ausgewertet werden kann. Zahlreiche öffentliche Organe sind an der Nutzung von Google Analytics interessiert oder setzen diese Software bereits ein.
Die datenschutzrechtliche Relevanz beim Einsatz von Google Analytics liegt darin, dass die IP-Adressen der Webseitenbesucher direkt an die Firma Google weitergeleitet werden. Eine Kontrolle darüber, wie und zu welchem Zweck die IP-Adressen weiterbearbeitet werden, ist für das öffentliche Organ nicht möglich. IP-Adressen sind Personendaten und deren Bearbeitung unterliegt den Rahmenbedingungen des IDG. Massgebend ist, dass das öffentliche Organ für die Datenbearbeitung verantwortlich bleibt, auch wenn die Informationen automatisch an Dritte, wie hier an Google, weitergeleitet werden. Ein vom Gesetz geforderter schriftlicher Vertrag muss sicherstellen, dass die Daten nur zum vorgesehenen Zweck analysiert, von anderen Daten getrennt bearbeitet und nach einer im Voraus definierten Frist gelöscht werden. Ungleich den Datenschutzbehörden in Deutschland ist es in der Schweiz nicht gelungen, sich mit Google über einen datenschutzkonformen Einsatz des Analysetools zu einigen. In unserem Nachbarland erhalten die User die Möglichkeit, Widerspruch gegen die Erfassung der Nutzerdaten einzulegen. Der Websitebetreiber kann verlangen, dass das letzte Oktett der IP-Adresse vor der Speicherung gelöscht wird und kann damit einen gesetzeskonformen Vertrag mit Google abschliessen.
Zum heutigen Zeitpunkt ist ein datenschutzkonformer Betrieb von Google Analytics in der Schweiz nicht möglich. Wollen kantonale Organe das Besucherverhalten ihrer Website erfassen, müssen sie eine Software einsetzen, welche die datenschutzrechtlichen Bedürfnisse erfüllen kann.
Die mit dem konkreten Anliegen um Prüfung der Software an den Datenschutzbeauftragten gelangte Hochschule hat Google Analytics von ihrer Website entfernt.

Vernehmlassungen

«Bei der Anpassung der verschiedenen gesetzlichen Grundlagen an das IDG besteht auch gegen Ende der fünfjährigen Übergangsfrist noch Handlungsbedarf.»

IDG schafft Transparenz bei Datenbearbeitungen

Das IDG räumt den öffentlichen Organen eine fünfjährige Übergangsfrist zur Anpassung der gesetzlichen Grundlagen für das Bearbeiten besonderer Personendaten ein. Der Handlungsbedarf wurde noch nicht in allen Bereichen erkannt und umgesetzt. Der zunehmenden Verwendung der Sozialversicherungsnummer in neuen Gesetzen ohne entsprechende Rahmenbedingungen steht der Datenschutzbeauftragte kritisch gegenüber.

Das IDG verlangt, dass für das Bearbeiten und Bekanntgeben von besonderen Personendaten eine hinreichend bestimmte Regelung in einem formellen Gesetz besteht. Fehlt eine solche Regelung, dürfen besondere Personendaten noch während fünf Jahren nach Inkrafttreten des IDG bearbeitet werden. Damit sollte dem Gesetzgeber genügend Zeit eingeräumt werden, gesetzgeberische Defizite zu beseitigen. Die Fünfjahresfrist endet am 30. September 2013. Vereinzelt wurden Gesetzesvorlagen zur Umsetzung dieser Anforderungen zuhanden des Kantonsrats verabschiedet oder in die Vernehmlassung geschickt. In einigen Bereichen wurde der Handlungsbedarf jedoch nicht erkannt und die gesetzgeberischen Aktivitäten lassen auf sich warten.

Der Datenschutzbeauftragte nimmt regelmässig Stellung zu kantonalen Gesetzesentwürfen und erstellt auch Mitberichte bei Gesetzgebungsvorhaben des Bundes. Dabei geht es ganz allgemein um datenschutzrechtlich relevante Entwicklungen sowie um angemessene und transparente Datenbearbeitungsbestimmungen.

Unerwünschte Verbreitung der AHV-Nummer

Im Berichtsjahr häuften sich Gesetzesänderungen, welche die Verwendung der Sozialversicherungsnummer (AHVN13) vorsahen. Die AHVN13 darf für administrative Zwecke verwendet werden, wenn ein Gesetz dies ausdrücklich vorsieht. Der Datenschutzbeauftragte lehnt es aber ab, die Sozialversicherungsnummer flächendeckend und ohne entsprechende Rahmenbedingungen in allen möglichen Verwaltungsbereichen als Personenidentifikator zu verwenden. Eine allgemeine Verbreitung und Verwendung, beispielsweise durch die Billag zur Erhebung der Radio- und Fernsehgebühren (Teilrevision des Radio- und Fernsehgesetzes) oder im Grundbuch (Teilrevision des Zivilgesetzbuches), wird unkontrollierbar. Hingegen kann einem Einsatz der AHVN13 in Bereichen, die einen Zusammenhang mit der Sozialversicherung aufweisen, wie beispielsweise der Personaladministration, zugestimmt werden.

Der Datenschutzbeauftragte hat 2012 unter anderem zu folgenden Gesetzgebungsprojekten Stellung bezogen:

Kanton

- Änderung Publikationsverordnung
- Bericht und Vereinbarung zur künftigen Zusammenarbeit zwischen Gemeinden und Kanton im Bereich E-Government
- Änderung des Polizeiorganisationsgesetzes und Abschluss einer Vereinbarung zwischen dem Kanton Zürich und der Stadt Zürich über Errichtung und Betrieb des Forensischen Instituts Zürich
- Ergänzungen des Sozialhilfegesetzes sowie des Gesetzes über Invalideneinrichtungen für erwachsene Personen und den Transport mobilitätsbehinderter Personen
- Änderung Personalgesetz (Fallbegleitung und PULS-ZH)
- Revision der Verordnung über den Gemeindehaushalt
- Verordnung über den elektronischen Zugriff der Kindes- und Erwachsenenschutzbehörden auf die Einwohnerregister
- Anpassung Gesetzgebung im Bereich der Bildungsdirektion an das IDG

Bund

- Teilrevision Radio- und Fernsehgesetz
- Teilrevision des Bundesgesetzes über die Ausländerinnen und Ausländer
- Ausdehnung der Rechtshilfe bei Fiskaldelikten (Teilrevision Rechtshilfegesetz, Übernahme von Zusatzprotokollen des Europarates)
- Revision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur
- Parlamentarische Initiative (09.430) betreffend Änderung Opferhilfegesetz (Schaffung wichtiger Informationsrechte des Opfers)
- Bundesgesetz über das Strafregister (Informationssystem VOSTRA)
- Änderung des Schweizerischen Zivilgesetzbuches betreffend Beurkundung Personenstand und Grundbuch

Bildungsdirektion passt Gesetzgebung an IDG an

Das IDG gibt den öffentlichen Organen ab 1. Oktober 2008 fünf Jahre Zeit, um das Bearbeiten von besonderen Personendaten mit Blick auf die datenschutzrechtlichen Anforderungen an eine hinreichend bestimmte gesetzliche Grundlage rechtskonform zu regeln. Die Bildungsdirektion hat 2012 eine umfassende Gesetzesvorlage in die Vernehmlassung geschickt.

Mit Inkrafttreten des IDG am 1. Oktober 2008 wurden die Anforderungen an das Bearbeiten von Personendaten dem Bedürfnis nach Transparenz angepasst. In Bezug auf das Bearbeiten von Personendaten wurden die Anforderungen gelockert, indem diese bearbeitet werden dürfen, wenn dies zur Erfüllung einer gesetzlich umschriebenen Aufgabe geeignet und erforderlich ist. Im Gegensatz dazu braucht es für das Bearbeiten von besonderen Personendaten eine hinreichend bestimmte Regelung in einem formellen Gesetz. Den öffentlichen Organen wurde eine Übergangsfrist von fünf Jahren gewährt, um die entsprechende gesetzliche Grundlage zu schaffen. Ziel dieser Anforderungen ist es, Bearbeitungen mit sensiblen Daten, also mit solchen, von denen eine erhöhte Gefahr von Persönlichkeitsverletzungen ausgeht, transparent zu gestalten. Die Betroffenen sollen nachvollziehen können, zu welchem Zweck der Staat besondere Personendaten bearbeitet und wem diese bekannt gegeben werden. Damit wird die Rechtssicherheit gestärkt.

Vor diesem Hintergrund hat die Bildungsdirektion 2012 eine umfassende Anpassung ihrer Rechtsgrundlagen in die Wege geleitet und die Gesetzesvorlage «Anpassung der Gesetzgebung im Bereich der Bildungsdirektion an das Gesetz über die Information und den Datenschutz» in die Vernehmlassung geschickt. Revidiert werden das Bildungsgesetz, das Volksschulgesetz, das Lehrpersonalgesetz, das Mittelschulgesetz, das Einführungsgesetz zum Bundesgesetz über die Berufsbildung, das Fachhochschulgesetz, das Universitätsgesetz, das Kinder- und Jugendhilfegesetz sowie das Gesetz über die Jugendheime und die Pflegekinderfürsorge.
Im Wesentlichen werden die Rahmenbedingungen des IDG für Datenbearbeitungen verankert, insbesondere explizite Regelungen für die konkreten Datenbearbeitungen wie beispielsweise die Verwendung der Versichertennummer der Alters- und Hinterlassenenversicherung (AHV) oder die Nutzung einer externen Datenbank zur Plagiatserkennung auf allen Bildungsstufen. Mehrheitlich finden sich auch Bestimmungen zur Amtshilfe und zur Datenbekanntgabe in den Gesetzesanpassungen, wie etwa der Informationsaustausch zwischen der Jugendanwaltschaft und den Bildungsinstitutionen bei der Eröffnung und dem Abschluss von Strafverfahren gegen Schülerinnen und Schüler wegen eines Verbrechens oder Vergehens.

Verordnung über den elektronischen Zugriff der Kindes- und Erwachsenenschutzbehörden (KESB) auf die Einwohnerregister

Das Einführungsgesetz zum Kindes- und Erwachsenenschutzrecht räumt den Kinder- und Erwachsenenschutzbehörden die Möglichkeit des Online-Zugriffs auf verschiedene Daten der Einwohnerregister der Gemeinden ein. Die Modalitäten des Abrufverfahrens werden in der dazugehörigen Verordnung geregelt. Der Datenschutzbeauftragte regte in seiner Stellungnahme die Aufnahme einer Bestimmung über den Zweck des Abrufverfahrens – die Prüfung der örtlichen Zuständigkeit – in die Verordnung an, da sich dieser aus der Gesetzesbestimmung nicht ergibt. In diesem Zusammenhang forderte er auch eine Präzisierung der Regelung des Zugriffs, nämlich dessen Beschränkung auf die Einwohnerregister jener Gemeinden, welche in die örtliche Zuständigkeit der jeweiligen KESB fallen. Des Weiteren beurteilte er die vorgesehene Aufbewahrungsfrist der elektronischen Protokolle über die erfolgten Zugriffe von fünf Jahren als zu lange. Die Aufbewahrung der Protokolle dient der Kontrolle, dass Abrufverfahren nicht missbräuchlich verwendet werden, weshalb eine Aufbewahrungsfrist von maximal zwölf Monaten genügt. Zudem verlangte er, die Löschung der Protokolle zu regeln. Schliesslich empfahl er, die Regelung der Einsichtnahme in die Protokolle um eine organisatorische Vorschrift zu ergänzen. Durch den Zugriff auf ein Einwohnerregister gibt die KESB die Information bekannt, dass die Person, über welche Daten abgerufen werden, in ein Verfahren involviert ist. Die Einsichtnahme in die Protokolle ist deshalb auf den IT-Verantwortlichen der Gemeinde und dessen Stellvertretung zu beschränken. Der Regierungsrat berücksichtigte die Hinweise und Anregungen des Datenschutzbeauftragten und erliess die Verordnung, die am 1. April 2013 in Kraft getreten ist.

Klare Rechtsgrundlagen im Personalgesetz geschaffen

Für die Datenbearbeitungen im Personal- und Lohnadministrationssystem (PULS-ZH), das auf Anfang 2011 eingeführt worden war, fehlten bisher hinreichend bestimmte Rechtsgrundlagen (siehe Tätigkeitsbericht 2010, Seite 13). Das Personalgesetz musste deshalb geändert werden. Die notwendigen Anpassungen wurden durch das Personalamt im Verlauf des Jahres 2011 erarbeitet und mit dem Datenschutzbeauftragten konsolidiert. Neu sollte das Personaldossier zudem ausschliesslich elektronisch geführt werden können. Auch Rekrutierungen sollten elektronisch abgewickelt werden können. Auf gesetzlicher Stufe war auch zu regeln, welche Datenkategorien in der Personaladministration bearbeitet werden, da es sich bei diesen Daten um besondere Personendaten im Sinne des IDG handelt. Darüber hinaus war auch die Fallbegleitung, das so genannte Case Management, festzulegen (siehe dazu auch Tätigkeitsbericht 2007, Seite 16). Klarheit in diesem Bereich schafften die neuen Bestimmungen über die Ziele und den Ablauf der Fallbegleitung sowie über die Voraussetzungen für Datenbearbeitungen. Zu den Gesetzesänderungen fand in der zweiten Hälfte 2012 eine Vernehmlassung statt. Der Datenschutzbeauftragte begrüsste in seiner Stellungnahme die geplanten Gesetzesanpassungen.

Teilrevision des Bundesgesetzes über die Ausländerinnen und Ausländer

Der Datenschutzbeauftragte nahm im Rahmen der Vernehmlassung zur Teilrevision des Bundesgesetzes über die Ausländerinnen und Ausländer zur Regelung des Passagier-Informationssystems (Advanced Passenger Informationssystem) Stellung. Das Passagier-Informationssystem wird vom Bundesamt für Migration (BFM) geführt und bezweckt die Verbesserung der Durchführung der Grenzkontrollen sowie die wirksamere Bekämpfung rechtswidriger Ein- und Durchreisen. Dazu kann das BFM Luftverkehrsunternehmen verpflichten, ihm oder der für die Grenzkontrollen zuständigen Behörde zu bestimmten Flügen Personendaten der beförderten Personen sowie Daten zum Flug zu melden. Diese Daten werden anschliessend automatisiert mit den Daten der schweizerischen und europäischen Fahndungssysteme, dem Zentralen Migrationsinformationssystem sowie der Interpol-Datenbank für gestohlene und verlorene Dokumente abgeglichen. Die Ergebnisse stehen den zuständigen Grenzkontrollbehörden zur Verfügung.
Der Datenschutzbeauftragte begrüsste die Schaffung einer gesetzlichen Grundlage, welche das BFM explizit ermächtigt, das Passagier-Informationssystem zu führen. Es stellt sich jedoch die Frage, ob ein solcher automatisierter Datenabgleich mit anderen Datenbanken verhältnismässig ist, denn jeder Fluggast wird anlass- und verdachtsunabhängig überprüft. Weiter ist unklar, ob das Verfahren schengenkonform ist und wie die Rechte Betroffener auf Einsicht, Berichtigung und Löschung umgesetzt werden sollen, denn das BFM hat in die Ergebnisse des automatisierten Abgleichs keine Einsicht.

Datenbearbeitung im Bereich der Eingliederung invalider Personen

Der Datenschutzbeauftragte nahm im Rahmen des Vernehmlassungsverfahrens zur Ergänzung des Gesetzes über Invalideneinrichtungen für erwachsene Personen und den Transport mobilitätsbehinderter Personen (IEG) sowie des Sozialhilfegesetzes (SHG) Stellung.
Das Finanzierungsmodell im Bereich der Eingliederung invalider Personen orientiert sich bezüglich der Höhe der Abgeltung am individuellen Betreuungsbedarf der invaliden Person. Für diese Bemessung sind besondere Personendaten erforderlich, welche Auskunft über die Art der Behinderung, den Rentenanspruch, die Einstufung der Hilflosigkeit und den individuellen Betreuungsbedarf geben. Das IDG schreibt für den Umgang mit solchen besonderen Personendaten eine Grundlage in einem formellen Gesetz vor. Die vorliegende Gesetzesänderung schafft in einem neuen § 18a die rechtliche Grundlage für die Führung einer Klientendokumentation durch die Einrichtungen sowie in einem neuen § 18b diejenigen für die Bearbeitung der Daten der Einrichtungen durch die zuständige Direktion. Damit sind die datenschutzrechtlichen Vorgaben einer hinreichend bestimmten, gesetzlichen Grundlage erfüllt. Mit den ergänzenden gesetzlichen Bestimmungen wird für die betroffenen Personen die notwendige Transparenz geschaffen, weshalb der Datenschutzbeauftragte den Gesetzesentwurf begrüsste.

«Die wirkungsvollste Kontrollmassnahme ist, Informationssicherheit im Arbeitsalltag zu leben.»

Kontrolle als Chance zur Minimierung von Risiken

Kontrolle ist das Eine, die Umsetzung der definierten Massnahmen das Andere. Sind Schwachstellen lokalisiert, können die Risiken durch die Umsetzung der Massnahmen minimiert werden. Massnahmen müssen deshalb periodisch überprüft, dem Schutzniveau angepasst und neu implementiert werden.

Informationssicherheit heisst, Informationen und Daten durch dem jeweiligen Schutzniveau angepasste organisatorische und technische Massnahmen zu schützen.

Das Erstellen der für das Umsetzen der Informationssicherheit notwendigen Dokumente benötigt Know-how und Ressourcen. Gemeinden und andere Institutionen, welche mit der Erfüllung öffentlicher Aufgaben betraut sind, wie beispielsweise Spitex-Organisationen, sind zum Teil auf externe Hilfe angewiesen, um das Notwendige vorzukehren. Um den Aufwand zu reduzieren und das fehlende Know-how auszugleichen, stehen auf der Website des Datenschutzbeauftragten www.datenschutz.ch Anleitungen, Vorlagen und Checklisten zur Verfügung. Diese sind an die unterschiedlichen Anforderungen grösserer und kleinerer öffentlicher Organe angepasst. Ohne grossen Aufwand können auf diese Weise die Sicherheitsdokumentation erstellt und die Massnahmen geplant werden. Parallel dazu kann ein Kurs besucht werden, in dem die Anwendung der Dokumente praxisorientiert vermittelt und direkt auf Anliegen der Betroffenen eingegangen wird.

Wichtiger noch als die Dokumentation ist es jedoch, Informationssicherheit im Arbeitsalltag zu leben. Die Mitarbeitenden sollten regelmässig sensibilisiert werden. Nur so können Sicherheitsrisiken eingegrenzt werden.

Im Rahmen der Kontrollen des Datenschutzbeauftragten, denen stets eine sorgfältige Risikoanalyse vorausgeht, werden nicht nur vorhandene Schwachstellen lokalisiert; das kontrollierte Organ profitiert auch von Informationen, die generell der Verbesserung des Datenschutzes und der Informationssicherheit dienen. Darüber hinaus können die öffentlichen Organe jederzeit und kostenlos eine Beratung durch die IKT-Experten des Datenschutzbeauftragten in Anspruch nehmen.

Vorabkontrollen werden immer wichtiger

Der Trend der elektronischen Datenbearbeitung geht nicht nur in Richtung immer grösser werdende Datenmengen. Auch möchte die Verwaltung immer häufiger neue Technologien mit zusätzlichen und umfassenderen Bearbeitungsmöglichkeiten verwenden. Das Instrument der Vorabkontrolle ist hier besonders gut geeignet, eine breit abgestützte Risikoabschätzung vorzunehmen.

Das elektronische Bearbeiten von Daten vereinfacht Vieles. Dennoch dürfen die datenschutzrechtlichen Rahmenbedingungen ob der Einfachheit und der Kostenvorteile, beispielsweise bei der Nutzung von Cloud Services, nicht vergessen werden. Vorabkontrollen ermöglichen es auf optimale Art und Weise, im Voraus die wesentlichen Faktoren zu bestimmen und eine datenschutzkonforme Datenbearbeitung zu planen.

2012 waren die Vorabkontrollen des Datenschutzbeauftragten vor allem beim Einsatz neuer Software notwendig. Dabei handelte es sich beispielsweise um die Frage der zentralen elektronischen Bewirtschaftung von Bewerbungen, der rein elektronischen Bearbeitung von Steuererklärungen und des Remote-Zugriffs auf Patientendaten durch Ärzte. Auch die Möglichkeit der Inanspruchnahme von «Software as a Service» kam zur Abklärung.

Vorerst muss bei Vorabkontrollen überprüft werden, ob die rechtlichen Grundlagen vorhanden sind. Eine genaue Analyse jedes einzelnen Projekts ist jedoch notwendig: So öffnen sich immer wieder neue Möglichkeiten der Datenbearbeitung, beispielsweise weil die Daten automatisierten Entscheiden, einem so genannten «Match-Scoring» zugeführt werden. Eine der 2012 durchgeführten Vorabkontrollen befasste sich mit dem Thema des «Bonitäts-Scoring». In diesem Fall werden Bonitätsprüfungen automatisiert durch Dritte ausgeführt. Die erhöhte Intransparenz und die Gefahr von Persönlichkeitsverletzungen durch eine solche Datenbearbeitung müssen durch zusätzliche datenschutzrechtliche Massnahmen ausgeglichen werden. Wesentlich für einen wirksamen Datenschutz sind die organisatorischen und technischen Massnahmen, wobei die Planung genauso wichtig ist wie die Umsetzung.

Werden Datenbearbeitungen zusätzlich durch externe Partner ausgeführt, ist ein klarer Vertrag, der alle wesentlichen Aspekte des Outsourcings regelt, die Voraussetzung für eine datenschutzkonforme Bearbeitung der Informationen. Eine nachträgliche Kontrolle der Umsetzung der Vertragsbestimmungen gibt dem öffentlichen Organ zusätzliche Sicherheit.

§ 10 IDG
§ 24 IDV

Elektronisches Steuerbüro nicht gesetzeskonform

Für eine ausschliesslich elektronische Führung aller Steuerakten einer Gemeinde ausserhalb der Systeme des kantonalen Steueramts fehlt zurzeit die gesetzliche Grundlage.

Eine Gemeinde plante, in der Abteilung Steuern ein Enterprise Content Management System einzuführen, das die papiergebundene durch eine elektronische Geschäftsverwaltung ablösen sollte. Der Datenschutzbeauftragte prüfte das Projekt im Rahmen einer Vorabkontrolle. Datenschutzrechtlicher Massstab der Prüfung war hauptsächlich die aktuelle gesetzliche Grundlage im Steuerbereich.

Gemäss den Bestimmungen des Steuergesetzes kann die Finanzdirektion über die elektronische Erfassung und Aufbewahrung von Steuererklärungen sowie weiterer Steuerakten durch die Gemeindesteuerämter und das Kantonale Steueramt Vorschriften erlassen. Sie kann ausserdem weitere Bestimmungen betreffend die Vernichtung der Steuererklärungen und weiterer Steuerakten nach der elektronischen Erfassung und die Weiterleitung der elektronisch erfassten Steuerdaten von den Gemeindesteuerämtern an das kantonale Steueramt festlegen.

Die Finanzdirektion hat in einer Weisung Vorschriften insbesondere in Bezug auf das Scannen und Vernichten der ordentlichen Steuerdaten erlassen. Am 1. Januar 2013 ist zudem die Verordnung über die elektronische Einreichung der Steuererklärung in Kraft getreten. Das geplante Projekt muss somit bei der Umsetzung die Anforderungen dieser Erlasse beachten. Was die übrigen Steuerakten betrifft, so bestehen diesbezüglich keine hinreichend bestimmten Regelungen für die elektronische Erfassung und Aufbewahrung oder Vernichtung der Originalakten. Diese Art der Bearbeitung ist somit nicht möglich, denn das Steuergesetz enthält eine Delegationsnorm, gemäss welcher die darin angeführten Datenbearbeitungen erst zulässig sind, wenn die Finanzdirektion konkretisierende Vorschriften erlassen hat.

Zusammenfassend bedeutet dies, dass für die Einführung eines elektronischen Systems im Bereich der Steuern in der vorgesehenen Form die gesetzliche Grundlage fehlt. Namentlich im Bereich der Einkommens-, Vermögens- sowie der Kapital- und Gewinnsteuern könnte dieses unter Beachtung der Rahmenbedingungen implementiert werden. Für die übrigen Steuerbereiche wie zum Beispiel die Erbschafts- und Schenkungssteuern kann die Gemeinde zwar eine elektronische Geschäftsverwaltung einführen, aber aufgrund der mangelnden Vorschriften der Finanzdirektion nicht die Führung der Papierdossiers durch diese elektronische Aktenführung ersetzen und die Originalakten vernichten.

Die anfragende Gemeinde hat in der Zwischenzeit kundgetan, die Weiterführung des Projekts unter den gegebenen Umständen zu überdenken.

§ 10 IDG
§ 24 IDV
§ 109d Steuergesetz

Automatisierte Auswahl von Bewerbungen

Der Einsatz einer Software, die eine zentrale Erfassung und Bearbeitung von Bewerbungen inklusive einer automatisierten Vorselektion ermöglicht, ist grundsätzlich zulässig. Voraussetzungen sind Transparenz in Bezug auf dieses «Scoring» und die Möglichkeit, Korrekturansprüche geltend zu machen.

Ein Spital plante, eine Software für Online-Rekrutierungen einzusetzen. Diese Software ermöglicht eine zentrale Bearbeitung von Bewerbungen inklusive der automatisierten Entscheide in Bezug auf eine Vorselektion der Bewerbenden. Das Spital bat den Datenschutzbeauftragten aufgrund der grossen Anzahl der Betroffenen und des Einsatzes von neuen Technologien um eine Vorabkontrolle.

Personalrechtliche Bestimmungen, die sich zur elektronischen Bearbeitung von Bewerbungen äussern, sind spärlich und erwähnen nicht explizit den Einsatz einer solchen Software.

Einzig in Bezug auf Mitarbeiterbeurteilungen besteht Klarheit, dass diese noch im Original aufbewahrt werden müssen. Mit Blick auf die Tatsache, dass keine zusätzliche als die bisher getätigte Datenbearbeitung erfolgt, und dass de lege ferenda Bestimmungen für eine kantonale E-Recruiting-Plattform in der Personalgesetzrevision vorgesehen sind, kann davon ausgegangen werden, dass ein elektronisches Bewerbungsverfahren von der Vollzugsverordnung zum Personalgesetz abgedeckt wird.

Wichtig ist, sicherzustellen, dass der Auftragnehmer, der diese Bearbeitung im Rahmen eines «Software as a service» anbietet, die Daten unter keinen Umständen für eigene oder andere Zwecke bearbeitet.

Bei einem automatisierten Entscheiden, einem sogenannten «Match Scoring», werden die für die zu besetzende Stelle unabdingbaren Kriterien festgelegt, wie beispielsweise ein Hochschulabschluss. Alle Bewerbenden ohne Hochschulabschluss würden demnach eine automatisiert erstellte Absage erhalten. Bei Entscheiden besteht die Gefahr, dass ungesicherte oder unkorrekte Aussagen über Personen bearbeitet werden. Da die Rechtmässigkeit, und insbesondere auch die Richtigkeit, dieser Entscheide durch betroffene Personen kaum überprüft werden können, sind zusätzliche Massnahmen umzusetzen. Die Bewerbenden sind auf dieses «Scoring» hinzuweisen und müssen bei einer Negativmeldung über die Herkunft des Resultats orientiert werden. Es ist sicherzustellen, dass nur «Muss-Kriterien» in ein solches Scoring einfliessen und Betroffene ihre Interessen geltend machen können. Dazu können auch Korrekturansprüche bei einer unzulässigen oder falschen Datenbasis oder einer falschen Berechnung gehören.

Durch den Auftraggeber zu treffende organisatorische und technische Massnahmen zum Schutz der Daten dürfen nicht fehlen, beispielsweise in Bezug auf die Sicherheit der Internetverbindung und der Webanwendung, auf die korrekte Vergabe der Zugriffsrechte und die Protokollierung.

§ 10 IDG
§ 24 IDV
§ 23 VVO

Informationssicherheit in Alters- und Pflegeheimen sowie Spitexorganisationen

2012 wurden erstmals Kontrollen bei Alters- und Pflegeheimen sowie Spitexorganisationen durchgeführt. Aufgrund der Resultate hat der Datenschutzbeauftragte umfangreiche Vorlagen, Beispiele und Checklisten zur Verbesserung der Sicherheit bereitgestellt.

Alters- und Pflegeheime sowie Spitexorganisationen bearbeiten mehrheitlich Patientendaten, die gemäss IDG als besondere Personendaten zu qualifizieren sind. Aufgrund ihres Risikopotenzials in Bezug auf Persönlichkeitsverletzungen unterliegen diese Daten erhöhten Anforderungen bei der Bearbeitung, namentlich auch bei der Bearbeitung durch Informationssysteme. Der Datenschutzbeauftragte hat 2012 ausgewählte Alters- und Pflegeheime sowie Spitexorganisationen kontrolliert. Geprüft wurden wie bei den Gemeinden die wichtigsten Massnahmen in den Bereichen Recht, Organisation und Technik. Die Resultate der Kontrollen zeigten, dass die Informationssicherheit nicht optimal eingehalten wurde. Die Defizite sind bei allen Organisationen auf mangelndes Know-how, geringe personelle Ressourcen und finanzielle Mittel sowie schwache Unterstützung durch die Auftragnehmenden in IKT-Sicherheitsfragen zurückzuführen. In Bezug auf die Zielvorgaben waren grösstenteils keine oder nur bescheidene Anstrengungen vorhanden. Weder existierte eine Leitlinie für Informationssicherheit noch eine Planung und Umsetzung von Massnahmen, ebenso wenig waren konkrete Weisungen an die Mitarbeitenden vorhanden. Die kostengünstigste und einfachste Massnahme, die Planung und Durchführung von Sensibilisierungsmassnahmen für IKT-Sicherheit, wurde nicht umgesetzt. Als Unterstützungsmassnahme hat der Datenschutzbeauftragte in der zweiten Jahreshälfte 2012 die für die grösseren Gemeinden erstellten Vorlagen, Beispiele und Checklisten an die Bedürfnisse der Alters- und Pflegeheime sowie der Spitexorganisationen angepasst. Damit können die erforderlichen Schritte schnell und effizient umgesetzt sowie teils auch an Auftragnehmer delegiert werden. Ein Kurs mit Fokus auf die Umsetzung der Massnahmen rundet die praxisorientierte Vermittlung von Fachwissen ab.

§ 34 lit. c IDG
§ 7 IDG

Zuständigkeit für Kontrollen in den Berufsschulen

Mit dem Ziel, die Anliegen des Datenschutzes in den Schulen nachhaltig zu diskutieren und zu verankern, wurden auch Kontrollen in mehreren Berufsschulen geplant und durchgeführt. Es zeigte sich, dass im Sicherheitsbereich teilweise Zielsetzungen und die dazugehörige Umsetzung von Massnahmen fehlten.

Ob alle Berufsschulen in den Geltungsbereich des IDG fallen, war nicht auf Anhieb klar. Die Berufsbildungsbereiche «berufliche Grundbildung», «höhere Berufsbildung» und «Weiterbildung» wurden daher einzeln mit Blick auf den Geltungsbereich des IDG überprüft.

Bei allen drei Bereichen ist grundsätzlich zwischen dem Angebot durch den Kanton oder durch private Unternehmen zu unterscheiden. Für kantonale Anbieter ist das IDG in der Regel anwendbar, es sei denn, diese nehmen am wirtschaftlichen Wettbewerb teil und handeln dabei nicht hoheitlich.

Werden Private mit der beruflichen Grundbildung mittels Leistungsvereinbarung beauftragt, so ist dies in vielen Bereichen staatlich reguliert und finanziert. Teilweise untersteht auch das Personal der nichtkantonalen Berufsfachschulen dem kantonalen Personalrecht, womit feststeht, dass die Anbieter der beruflichen Grundbildung öffentliche Organe im Sinne des IDG sind.

Bei der höheren Berufsbildung schliesslich ist zwischen den vorbereitenden Kursen für eidgenössische Berufs- und Fachprüfungen und den höheren Fachschulen zu unterscheiden. Werden die Kurse durch Private angeboten oder solche Fachschulen durch Private geführt, ist anhand einschlägiger Kriterien (gesetzlicher Auftrag, Finanzierung, staatliche Aufsicht usw.) im Einzelfall zu prüfen, ob die Voraussetzungen für eine Qualifikation als öffentliches Organ und somit die Geltung des IDG vorliegen. Dasselbe gilt für die Anbieter von berufsorientierten Weiterbildungen.

Die Resultate der Kontrollen zeigen, dass wenn Grundlagendokumente wie die Leitlinie zur Informationssicherheit und das Sicherheitskonzept einmal erstellt sind, sich die Umsetzung der Massnahmen als logische Abfolge gestaltet. Erstere fehlten teilweise bei den kontrollierten Berufsschulen. Wichtiger noch als diese Dokumente ist aber die konkrete Umsetzung der Sicherheitsmassnahmen. Hier besteht grosser Handlungsbedarf. Als Beispiel ist die regelmässige Sensibilisierung betreffend Datenschutz und Informationssicherheit zu nennen (Informationen über sichere Passwortbildung, Hinweis auf Risiken etc.) Weiter wurde dem Schutz der Daten auf mobilen Geräten wie zum Beispiel USB-Sticks oder Smartphones zu wenig Beachtung geschenkt.

§ 3 Abs. 1 lit. c IDG
§ 34 lit. c IDG

Kontakt

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

Impressum

Herausgeber: Datenschutzbeauftragter des Kantons Zürich, Postfach, 8090 Zürich
Korrektorat: Text Control, Zürich
Layout: René Habermacher, Visuelle Gestaltung, Flurstrasse 50, 8048 Zürich
Druck: Kantonale Drucksachen- & Materialzentrale KDMZ, Zürich
Auflage: 1000

ISSN 1422-5816

dsb

datenschutzbeauftragter
kanton zürich

www.datenschutz.ch

Datenschutz mit Qualität