dsb

datenschutzbeauftragter
kanton zürich

2015

Tätigkeitsbericht

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 2015 bis und mit 31. Dezember 2015 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, März 2016

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

«Mit der Vorabkontrolle wird sichergestellt, dass bei Datenbearbeitungsvorhaben mit besonders grossen Risiken für die Rechte und Freiheiten der Bürgerinnen und Bürger angemessene Schutzvorkehrungen getroffen werden.»

Inhaltsverzeichnis

Kontrollen und Vorabkontrollen

Information und Weiterbildung

Ausblick

Datenschutzbeauftragter Kanton Zürich

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

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

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

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

«Ein heimliches Ausspähen von Computer- oder Kommunikationsaktivitäten stellt einen schweren Eingriff in das verfassungsmässige Recht auf persönliche Freiheit dar.»

Datenschutz ist Prävention

Das Informations- und Datenschutzgesetz (IDG) sieht verschiedene Instrumente zur präventiven Gewährleistung des Datenschutzes vor. Dazu gehört die Pflicht der öffentlichen Organe zur Vorabkontrolle bestimmter Datenbearbeitungsvorhaben.

Die Vorabkontrolle ist das wichtigste Instrument des präventiven Datenschutzes. Öffentliche Organe haben beabsichtigte Datenbearbeitungen dem Datenschutzbeauftragten zu einer Vorprüfung zu unterbreiten, wenn besondere Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen. Die Verordnung zum Informations- und Datenschutzgesetz (IDV) konkretisiert dabei die Voraussetzungen für die Vorabkontrolle. «Besondere Risiken» liegen insbesondere vor, wenn

- Online-Zugriffe auf Personendaten vorgesehen sind,
- eine Vielzahl von besonderen Personendaten erhoben werden,
- neue Technologien zum Einsatz gelangen,
- verschiedene öffentliche Organe an einer Datenbearbeitung beteiligt sind,
- eine grosse Anzahl Personen betroffen sind.

Diese Aufzählung ist nicht abschliessend, ortet die Risiken aber im Wesentlichen in den Bereichen Technologie («neu», «online»), Datenkategorie («Sensitivität») und Umfang («verschiedene» öffentliche Organe, «grosse» Anzahl Personen). Damit haben die öffentlichen Organe die Leitlinien, wann ein Projekt zur Vorprüfung vorgelegt werden muss.

Unvollständige Vorabkontrollen

Trotz dieser klaren Voraussetzungen gelangen nicht alle vorabkontrollpflichtigen Datenbearbeitungsvorhaben zum Datenschutzbeauftragten. Die Gründe hierfür mögen unterschiedlich sein – ob Nachlässigkeit oder bewusste Umgehung der Vorabkontrolle, sei dahingestellt. Vereitelt werden dadurch aber eine transparente Datenbearbeitung und eine angemessene Behandlung der rechtlichen, technischen und organisatorischen Risiken. Erst im Nachhinein das Vorhaben datenschutzkonform zu gestalten, setzt die Bürgerinnen und Bürger unnötigen Risiken für ihre Privatsphäre aus und bedeutet für das öffentliche Organ einen nicht abschätzbaren Zusatzaufwand, abgesehen vom Vertrauensverlust bei einer Datenschutzpanne.

Bei einer Vorabkontrolle prüft der Datenschutzbeauftragte, ob die beabsichtigte Datenbearbeitung rechtlich zulässig ist und ob angemessene organisatorische und technische Massnahmen für die Sicherheit der Daten getroffen werden. Bestehen keine ausreichenden Rechtsgrundlagen für die Datenbearbeitung, kann er konkrete Vorschläge für zu schaffende rechtliche Rahmenbedingungen machen. Ebenso kann er organisatorische und technische Sicherheitsmassnahmen vorschlagen.

Die Prüfung erfolgt aufgrund der vom öffentlichen Organ vorgelegten Unterlagen, die allenfalls während der Prüfung zu ergänzen sind. Der Datenschutzbeauftragte stellt den öffentlichen Organen für das Vorabkontrollverfahren ein Merkblatt für das Vorgehen zur Verfügung.

Feststellungen im Kontrollbericht

Der Datenschutzbeauftragte schliesst das Verfahren mit einem Kontrollbericht ab. Soweit es sich im Verlauf des Verfahrens herausstellt, dass die Datenbearbeitung nicht der Vorabkontrollpflicht unterliegt, gibt er seine Feststellungen im Rahmen einer Beratung weiter. Das Vorhaben kann generell als datenschutzkonform bezeichnet werden, oder es können grössere oder kleinere Massnahmen vorgeschlagen werden.

Der Prüfungsbericht wird dem öffentlichen Organ innert angemessener Frist zugestellt. Dieses ist dabei frei, wie es mit den Feststellungen im Bericht umgehen will. So können Modifikationen am Vorhaben erfolgen oder neue rechtliche Grundlagen geschaffen werden. Technische Lösungen können angepasst werden, um aufwändige Sicherheitsmassnahmen zu vermeiden.

Sofern bereits im Voraus angemessene rechtliche Grundlagen für das Vorhaben geschaffen werden oder wenn der Datenschutzbeauftragte in der Projektorganisation mitwirkt, kann auf eine Vorabkontrolle verzichtet werden.

Vertrauensbildende Vorabkontrolle

Legt ein öffentliches Organ ein Vorhaben nicht zur Vorabkontrolle vor oder verweigert es die Vorabkontrolle trotz Aufforderung, hat der Datenschutzbeauftragte kein Rechtsmittel, um diese Prüfung durchzusetzen. Er kann lediglich bei konkreten Datenbearbeitungen eine Verletzung von Datenschutzvorschriften mittels einer Empfehlung allenfalls gerichtlich klären lassen.

Mit dem Instrument der Vorabkontrolle hat der Gesetzgeber die Bedeutung des präventiven Datenschutzes unterstrichen, um damit die Bildung von Vertrauen in die risikohaften Vorhaben der öffentlichen Organe zu stärken.

Fehlende Vorabklärungen

Besonders sensitive Personendaten werden im Polizeibereich und im Gesundheitsbereich bearbeitet. Das Fehlen von Vorabkontrollen führt zu offenen Fragen (Seiten 10 und 11) oder zu offensichtlichen Lücken im Bereich der Informationssicherheit, die erst im Nachhinein bei Kontrollen festgestellt werden können (Seiten 37 und 38).

Trojaner ausser Kontrolle

Die Kantonspolizei setzt unter der Bezeichnung «Staatstrojaner» oder «Government Software» Spionagesoftware ein, die heimlich Programme, Dateien, E-Mails und mehr ausspionieren kann. Diese Technologie wurde dem Datenschutzbeauftragten nicht zur Vorabkontrolle unterbreitet.

Im Sommer 2015 wurde bekannt, dass die Kantonspolizei ein GovWare-Programm beschafft hatte – dies, nachdem der Lieferant der Kantonspolizei selbst Opfer eines Hacking-Angriffs geworden war und Unterlagen über die Beschaffung auf dem Portal Wikileaks veröffentlicht worden waren.

Was ist ein «Staatstrojaner»?

Ein sogenannter «Staatstrojaner» ist eine Software, die es den Behörden ermöglicht, verdeckt auf die Internetkommunikation eines Computers oder Handys zuzugreifen und diese zu überwachen. Die Software wird ohne das Wissen der Benutzerin oder des Benutzers vom Überwachenden entweder via Internet oder direkt auf dem Computer installiert. Solche Software wird auch «Government Software» (GovWare) genannt. GovWare kann nicht nur die Internetkommunikation überwachen, sondern je nach Programmierung weitergehende Überwachungsfunktionen übernehmen und sogar das Gerät als solches manipulieren. GovWare vermag unter Umständen auch die Webcam eines Gerätes einzuschalten und so einen Raum in Bild und Ton vollständig zu überwachen.

Möglichkeiten von GovWare:

- Überwachung der Internetkommunikation (Internettelefonie, Messaging)
- Ausführen von Anwendungen
- Anfertigen von Screenshots
- Manipulation von Dateien und Programmen
- Inbetriebnahme von Webcam und Mikrofon
- Registrierung jeglicher Eingaben (Key-Logger-Funktionalität) inklusive Passworteingaben

All diese Vorgänge erfolgen heimlich, das heisst, sie sind für die Userin oder den User nicht erkennbar. Sofern die GovWare gut programmiert ist, wird sie weder von Antiviren- noch von Antispyware- noch von Intrusion-Detection-Programmen erkannt. GovWare übermittelt die ausgespähten Informationen unbemerkt an eine «Kommandozentrale», den kontrollierenden Server.

Vorabkontrolle

Das öffentliche Organ unterbreitet eine beabsichtigte Bearbeitung von Personendaten vorab der oder dem Beauftragten für den Datenschutz zur Prüfung (§ 10 IDG).

Eingriff in die Privatsphäre

Ein heimliches Ausspähen von Computer- oder Kommunikationsaktivitäten durch eine staatliche Stelle stellt einen schweren Eingriff in das verfassungsmässige Recht auf persönliche Freiheit und Datenschutz dar. Ein solcher Einschnitt ist nur innerhalb sehr enger Grenzen zulässig. Da insbesondere die technologische Entwicklung rasch voranschreitet und neue Möglichkeiten bietet, sieht das IDG vor, dass eine geplante Datenbearbeitung, die besondere Risiken für die Rechte und Freiheiten von betroffenen Personen darstellt, dem Datenschutzbeauftragten vorab zur Prüfung unterbreitet wird (siehe Kasten «Vorabkontrolle»).

Fragen an Kantonspolizei und Sicherheitsdirektion

Der Datenschutzbeauftragte wandte sich an die Kantonspolizei und verlangte, die GovWare einer Vorabkontrolle zu unterziehen. Die Kantonspolizei verneinte die Vorabkontrollpflicht, da der Einsatz solcher Software in der Strafprozessordnung geregelt und das IDG im Bereich des Strafverfahrens nicht anwendbar sei. Beiden Argumenten konnte der DSB nicht beipflichten, weshalb eine erneute Aufforderung zur Vorabkontrolle erging, was von der Kantonspolizei jedoch wiederum abgelehnt wurde.

Der Datenschutzbeauftragte gelangte in der Folge an die Sicherheitsdirektion und verlangte eine Aussprache. Nebst dem Einsatz von GovWare setzt die Kantonspolizei vermehrt auch neue Technologien ein, wie Videokameras in Polizeifahrzeugen, IMSI-Catcher (International Mobile Subscriber Identity Catcher zur Ortung und Abhörung von Smartphonenutzenden) usw. Die Frage, ob dies unkontrolliert und ohne zusätzliche Massnahmen zur Wahrung des Persönlichkeitsschutzes von unbeteiligten und unverdächtigen Personen möglich sein soll, ist grundsätzlicher Art. Bis zum Redaktionsschluss des vorliegenden Tätigkeitsberichts konnten die offenen Fragen mit der Sicherheitsdirektion noch nicht geklärt werden.

Auch die Geschäftsprüfungskommission (GPK) des Kantonsrates befasste sich mit der Angelegenheit und setzte dazu eine Subkommission ein. Der Datenschutzbeauftragte gab der Subkommission der GPK anlässlich einer Sitzung Auskunft über die Rechtslage und das Vorgehen.

§ 10 IDG
§ 24 IDV

Konstante Auslastung der Ressourcen

Mit den im Kontinuierlichen Entwicklungs- und Finanzplan (KEF) aufgeführten Indikatoren und Messgrössen werden für den Datenschutzbeauftragten Leistungsmerkmale ausgewiesen, die die Erfüllung der gesetzlichen Aufgaben wesentlich beeinflussen. Die Zahlen für 2015 bedeuten eine konstante Auslastung der Ressourcen und eine Beschränkung der gesetzlichen Aufgaben nach Prioritäten.

Damit genügend Ressourcen für die anderen Tätigkeiten zur Verfügung stehen, soll der Anteil Beratungen von Privatpersonen eine gewisse Anzahl nicht überschreiten. Mit den bestehenden Ressourcen lassen sich zirka 500 Beratungen pro Jahr bewältigen. Dabei handelt es sich mehrheitlich um Kurzberatungen, die sich telefonisch oder mittels E-Mail erledigen lassen. Im Jahre 2015 erfolgten 451 solcher Beratungen, was den Zielvorgaben entspricht.

Es sind auch viele Gesetzgebungsvorhaben zu prüfen, die sich im Nachhinein als nicht datenschutzrelevant erweisen oder bereits datenschutzkonform ausgestaltet sind, so dass sich eine Stellungnahme erübrigt. Die wichtigen und zeitintensiven Vernehmlassungen werden als Richtgrösse ausgewiesen. Die vorgesehene Anzahl von 18 wurde im Jahre 2015 mit 23 Vernehmlassungen um über einen Viertel überschritten.

Als Richtgrösse für das Jahr 2015 waren 40 Kontrollen vorgesehen. Dank der Standardisierung bedeutet dies eine Verdoppelung gegenüber dem Vorjahr. Die Zielvorgabe konnte mit 35 Kontrollen nicht ganz erreicht werden.

Aufgrund der beschränkten Ressourcen ist das Aus- und Weiterbildungsangebot für öffentliche Organe auf 20 Halbtage beschränkt. Im Jahre 2015 konnten 17 Angebote realisiert werden. Ausbildungsangebote in Form von fachspezifischen Referaten werden dabei nicht mitgezählt.

Neben den Leistungsindikatoren werden im KEF auch zwei Wirkungsindikatoren ausgewiesen. Dabei wird gemessen, wie die anlässlich von Kontrollen ausgesprochenen Hinweise von den öffentlichen Organen umgesetzt werden. In der Regel wird diesen eine Frist zu deren Umsetzung auferlegt. Während als Jahresziel eine Umsetzung von mindestens 60 Prozent der Hinweise angestrebt wurde, waren es effektiv nur rund 15 Prozent. Von den 85 anlässlich von Kontrollen ausgesprochenen Hinweisen wurden nur 13 umgesetzt. Dem Datenschutzbeauftragten fehlen die Ressourcen, um die Nachkontrollen zu verstärken und damit punkto Informationssicherheit eine höhere Wirkung zu erzielen. Als weiterer Wirkungsindikator werden die Besuche auf der Website gezählt. Mit rund 30 000 Besuchen im Jahr 2015 liegt der Wert unter den Erwartungen. Wegen eines neuen Tools mussten die Werte des KEF angepasst werden. Die Zielgrösse ist mindestens 40 000 Besuche, was weitere Massnahmen braucht, um die Attraktivität der Website zu verbessern.

Beratung

Der DSB berät öffentliche Organe und Privatpersonen in Fragen des Datenschutzes und der Informationssicherheit. Die Beratung erfolgt persönlich, telefonisch, per E-Mail oder schriftlich. Der Leistungsindikator im KEF misst die getätigten Beratungen von Privatpersonen.

KEF	500
2015	451

Vernehmlassungen

Der DSB beurteilt Entwürfe von Erlassen und Vorhaben im Gesetzgebungsverfahren mit Bezug zu Datenschutz und/oder Informationssicherheit. Dazu verfasst er Vernehmlassungsantworten, Stellungnahmen und Mitberichte. Der Leistungsindikator im KEF gibt Auskunft über die eingereichten Vernehmlassungsantworten, Stellungnahmen und Mitberichte.

KEF	18
2015	23

Weiterbildung und Information

Der DSB bietet Aus- und Weiterbildungen im Bereich des Datenschutzes und der Informationssicherheit an. Dies erfolgt in der Form von internen oder externen Seminaren, Kursen, Workshops, Web-Trainingsprogrammen und Referaten. Der Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote für öffentliche Organe.

KEF	20
2015	17

Kontrollen

Der DSB kontrolliert die Anwendung der rechtlichen, technischen und organisatorischen Vorschriften über den Datenschutz und die Informationssicherheit durch die öffentlichen Organe. Dazu führt er Datenschutz-Reviews, Kontrollen auf Anlass sowie technische Kontrollen durch. Der Leistungsindikator im KEF gibt Auskunft über die realisierten Kontrollen.

KEF	40
2015	35

Öffentlichkeitsprinzip und Aufsicht

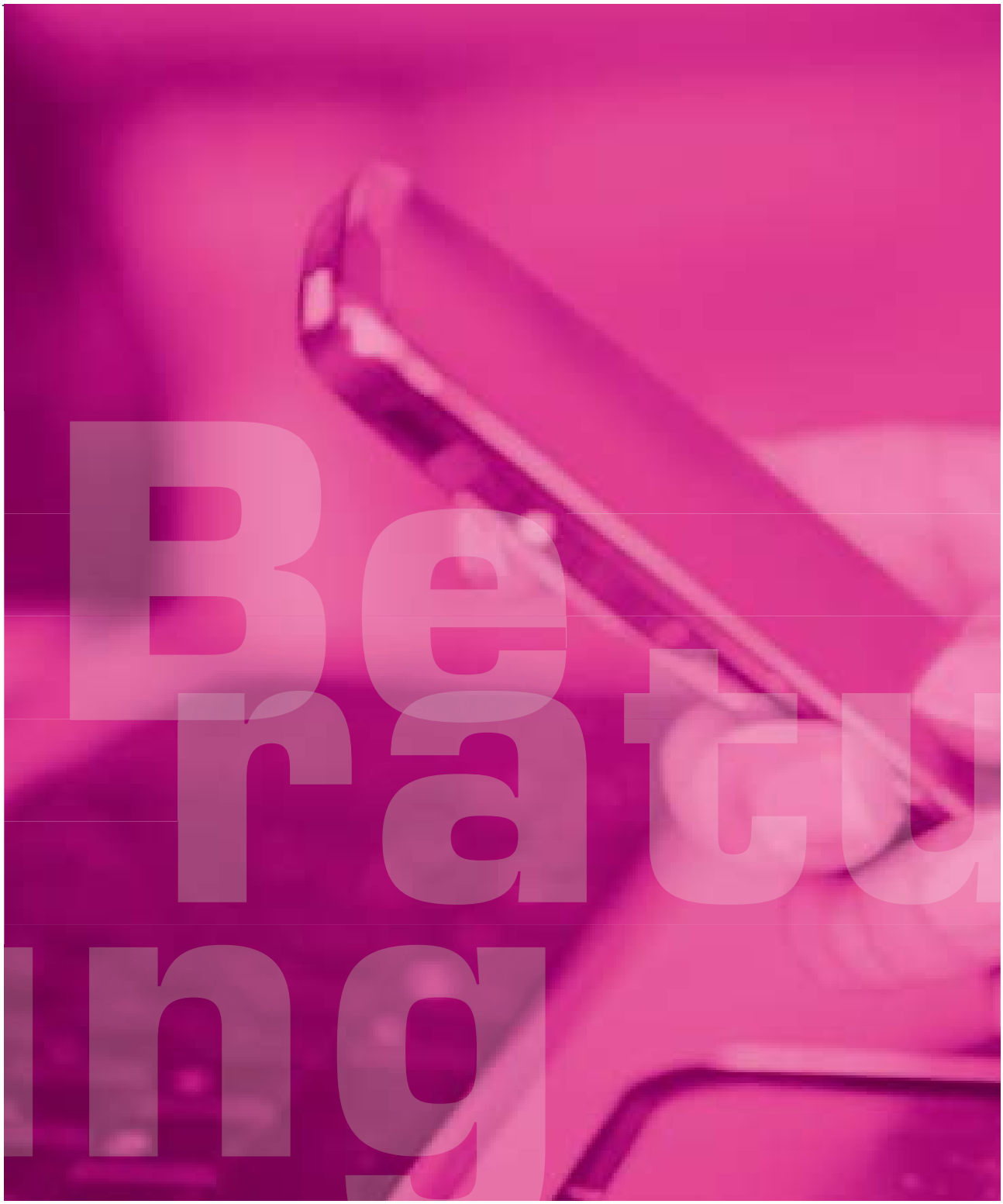
Zur Halbzeit der Evaluation der Wirkung des Informations- und Datenschutzgesetzes (IDG), welche von 2013 bis 2017 durchgeführt wird, zeigt sich Handlungsbedarf in verschiedenen Punkten.

Die Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) hatte im Jahr 2012 für den Datenschutzbeauftragten ein Konzept zur Evaluation des IDG entwickelt (siehe Tätigkeitsbericht 2012, Seite 12). Das Konzept sieht die Umsetzung in vier Teilschritten mit verschiedenen Evaluationsschwerpunkten sowie einer Evaluationssynthese vor.

Die Umsetzung startete 2013 mit einer Bevölkerungsbefragung. Evaluiert wurde damit das Thema der Sensibilisierung der Bevölkerung hinsichtlich Datenschutz und Öffentlichkeitsprinzip (siehe Tätigkeitsbericht 2013, Seite 14 ff.). In einem zweiten Teilschritt wurde das Thema der Gesetzmässigkeit von Datenbearbeitungen näher betrachtet (siehe Tätigkeitsbericht 2014, Seite 19 ff.).

Die Zwischenbilanz zeigt auf, dass das IDG grundsätzlich Wirkungen entfaltet hat. Allerdings traten auch einzelne Schwächen auf. So offenbarte sich, dass das Thema Öffentlichkeitsprinzip und Informationszugangsrecht in der Bevölkerung noch wenig bekannt ist. Auch die Gesetzgebung hinkt den Anforderungen des IDG teilweise hinterher. Trotz einiger Bemühungen zur Schaffung von transparenteren Normen über Datenbearbeitungen besteht mancherorts noch Handlungsbedarf. Die beiden weiteren Teilschritte der Evaluation befassen sich mit der Umsetzung des Öffentlichkeitsprinzips durch die Verwaltung sowie mit der Aufsicht. Die Umsetzung des Öffentlichkeitsprinzips wird daran gemessen, ob verwaltungsintern Abläufe und Handlungsanweisungen für den Umgang mit Informationszugangsgesuchen bestehen, Verantwortlichkeiten geregelt sind und proaktiv über wichtige Ereignisse und Themen informiert wird. Bei der Evaluation der Aufsicht als letztem Teilschritt stehen die Instrumente, Kompetenzen und Verfahren der Aufsicht in Datenschutz und Öffentlichkeitsprinzip im Fokus.

Abschliessend werden die Ergebnisse der vier Teilevaluationen und allenfalls weiterer Aspekte in einer Synthese zusammengefasst, aus welcher Schlussfolgerungen und ein allfälliger Handlungsbedarf abzuleiten sein werden. Die Ergebnisse der einzelnen Teilschritte und der Evaluationssynthese werden jeweils auf der Website des Datenschutzbeauftragten veröffentlicht (Rubrik «Veröffentlichungen» → «Evaluation»).



«Die Videoüberwachung muss so ausgestaltet werden, dass keine permanente Überwachung der Mitarbeitenden erfolgt.»

Komplexe Beratungen im Vordergrund

Die Beratungstätigkeit gehört zu den Hauptaufgaben des Datenschutzbeauftragten. Für eine Beratung in datenschutzrechtlichen Fragen können sich sowohl die öffentlichen Organe wie auch Privatpersonen an den Datenschutzbeauftragten wenden (§ 34 lit. a und b IDG). Je nach Sachverhalt erfolgt die Beratung mündlich oder schriftlich oder der Datenschutzbeauftragte verweist auf seine einschlägigen Publikationen, Merkblätter und Checklisten auf seiner Website.

Damit genügend Ressourcen für die anderen Tätigkeiten zur Verfügung stehen, soll der Anteil Beratungen von Privatpersonen eine gewisse Anzahl nicht überschreiten. Mit den bestehenden Ressourcen lassen sich zirka 500 Beratungen pro Jahr bewältigen. Dabei handelt es sich mehrheitlich um Kurzberatungen, die sich telefonisch oder mittels E-Mail erledigen lassen. Im Jahr 2015 erfolgten 451 solcher Beratungen, was den Zielvorgaben entspricht.

Der DSB berät öffentliche Organe und Privatpersonen in Fragen des Datenschutzes und der Informationssicherheit. Die Beratung erfolgt persönlich, telefonisch, per E-Mail oder schriftlich. Der Leistungsindikator im KEF misst die getätigten Beratungen von Privatpersonen.

KEF	500
2015	451

Die Beratungen decken ein breites Themenspektrum ab. Bei den öffentlichen Organen handelt es sich vielfach um grundlegende Fragen bei sensitiven Datenbearbeitungen wie dem Datenaustausch im Schul- oder Sozialbereich. Einzelpersonen interessieren sich für die datenschutzrechtliche Einschätzung bei konkreten Individualfällen und eine Beratung für das weitere Vorgehen.

Immer häufiger beziehen sich Beratungen auch auf den Einsatz von neuen Technologien und Anwendungen wie Plagiatserkennungs- und Analysesoftware oder die Verwendung einheitlicher elektronischer Identitäten.

Insgesamt hat der Anteil der Komplexität der datenschutzrechtlichen Fragestellungen in der Beratungstätigkeit zugenommen, da einerseits immer mehr Fälle an den Datenschutzbeauftragten gelangen und andererseits die einfacheren Sachverhalte von den öffentlichen Organen eigenständig aufgrund der Informationen auf der Website des Datenschutzbeauftragten beantwortet werden können.

Die Beratungstätigkeit bleibt damit ein wesentlicher Pfeiler der gesetzlichen Aufgaben des Datenschutzbeauftragten.

01
Verhinderung der Amtsblatt-Indexierung für Suchmaschinen

Eine Privatperson wandte sich an den Datenschutzbeauftragten, da bei Eingabe ihres Namens in der Internet-Suchmaschine Google eine im Amtsblatt publizierte amtliche Mitteilung als Treffer erschien, obwohl die Mitteilung über die Suchfunktion auf der Website des Amtsblattes nicht mehr auffindbar war. Diese Suchfunktion steht während einer bestimmten Dauer ab der Veröffentlichung einer amtlichen Mitteilung zur Verfügung, da der Zweck der Publikation nach Ablauf dieser Frist in der Regel erreicht ist und eine zeitlich unbeschränkte Suchmöglichkeit unverhältnismässig wäre.
Durch den Datenschutzbeauftragten vorgenommene Stichproben zeigten, dass auch in anderen Fällen amtliche Mitteilungen nach Ablauf der Suchfrist über die Internet-Suchmaschine Google auffindbar waren. Die Analyse ergab, dass die Online-Ausgaben des Amtsblattes für Suchmaschinen indexiert waren. Durch die Indexierung wurde die Vorschrift unterlaufen, wonach die Suchfunktion auf der Website des Amtsblattes nur während einer gewissen Dauer zur Verfügung steht. Der Datenschutzbeauftragte wandte sich deshalb an die für die Herausgabe des Amtsblattes zuständige Staatskanzlei und bat diese, Massnahmen in die Wege zu leiten, um die Indexierung durch Suchmaschinen zu verhindern.
In der Folge veranlasste die Staatskanzlei mit beratender Unterstützung durch den Datenschutzbeauftragten die Umsetzung von Massnahmen, welche die Indexierung der Online-Ausgaben des Amtsblattes für Suchmaschinen wirksam verhindern. Heute sind nicht nur amtliche Mitteilungen, deren Frist für die Suchfunktion auf der Website des Amtsblattes abgelaufen ist, nicht mehr über Suchmaschinen auffindbar, sondern auch sämtliche amtlichen Mitteilungen. Damit konnte dem Grundsatz der Verhältnismässigkeit mit technischen Massnahmen Nachachtung verschafft werden.

§ 8 IDG
§ 9b Publikationsverordnung

02
Ablehnende Verfügung bei Datensperre

Eine Gemeinde wandte sich mit der Frage an den Datenschutzbeauftragten, wie ein rekursfähiger Beschluss zu begründen sei, wenn das Bestehen einer Datensperre nicht angegeben werden soll.
Jeder Einwohner einer Zürcher Gemeinde kann gegen die voraussetzungslose Bekanntgabe von Personendaten aus dem Einwohnerregister an Private eine Datensperre errichten. Eine Durchbrechung dieser Sperre ist unter bestimmten Voraussetzungen möglich. Durchbricht die Einwohnerkontrolle die Datensperre nicht und gibt die Daten nicht bekannt, teilt sie dies der anfragenden Person in einer Verfügung mit. Bei der Formulierung dieser Verfügung ist zu beachten, dass keine Informationen zur betroffenen Person bekanntgegeben werden. Es darf insbesondere nicht aus der Verfügung hervorgehen, ob die Person in der Gemeinde wohnt oder nicht. Der Datenschutzbeauftragte hat deshalb folgende mögliche Formulierung vorgeschlagen: «Zu dieser Person können wir Ihnen keine Auskunft erteilen, da entweder das Einwohnerregister keine Angaben enthält oder eine Datensperre gemäss § 22 IDG besteht.»

§ 22 IDG
§ 18 MERG

03
Videoüberwachung im Schwimmbad

Der Datenschutzbeauftragte hat sich im Berichtsjahr mit Fragen bezüglich Videoüberwachung in Schwimmbädern mehrerer Gemeinden befasst.
Eine Gemeinde fragte den Datenschutzbeauftragten für die Prüfung ihres Reglements zur Videoüberwachung im Hallenbad an. Dabei wies der Datenschutzbeauftragte darauf hin, dass eine Auswertung der Aufzeichnungen nur bei einem konkreten Anlass zulässig ist. Wenn beispielsweise eine Widerhandlung festgestellt wird, können die Aufnahmen gesichtet und die betroffenen Teile der Aufzeichnungen der Polizei zur weiteren Bearbeitung übergeben werden. Zudem machte der Datenschutzbeauftragte darauf aufmerksam, dass die Videoüberwachung so auszugestalten ist, dass keine permanente Überwachung der Mitarbeitenden stattfindet. Nachdem sich sowohl die Gemeinde als auch betroffene Badegäste bezüglich einer Eingangskontrolle in ein Schwimmbad an den Datenschutzbeauftragten gewandt hatten, liess sich dieser die Eingangskontrolle vor Ort zeigen. Bei der besichtigten Installation wird beim Eingang bei Hinhalten der Eintrittskarte an ein Lesegerät auf einem Bildschirm die Fotografie der eintretenden Person gezeigt und dann das Drehkreuz freigeschaltet. Die Anzeige der Fotografie dient der Kontrolle, ob die eintretende Person mit der Inhaberin oder dem Inhaber der Eintrittskarte übereinstimmt. Weil sich die Bildschirme unmittelbar beim Kontrollpunkt befinden, nicht unverhältnismässig gross sind, lediglich die Fotografie (und keine weiteren Daten zur Person) angezeigt wird und die Anzeige nach wenigen Sekunden wieder erlischt, kam der Datenschutzbeauftragte zum Schluss, dass keine datenschutzrechtlich unzulässigen Datenbearbeitungen stattfinden.
Ein Mitarbeiter eines Schwimmbades wandte sich wegen einer Videoüberwachung im Kassenhaus an den Datenschutzbeauftragten. Das Kassenhaus dient dem Mitarbeiter als Arbeitsplatz. Zudem werden in diesem Raum auch Badegäste verarztet.
Der Datenschutzbeauftragte nahm mit der Gemeinde Kontakt auf und wies insbesondere auf den Grundsatz der Verhältnismässigkeit hin, welcher – neben dem Vorliegen einer gesetzlichen Grundlage für die Videoüberwachung – eingehalten werden muss. Im Rahmen des Bearbeitungszwecks, beispielsweise die Verhinderung von Einbrüchen während der Nacht, müssen die Betriebszeiten der Kamera eingeschränkt werden. Es darf keine dauerhafte Überwachung der Mitarbeitenden stattfinden und die Intimsphäre der Badegäste, die sich verarzten lassen und sich dafür allenfalls ausziehen müssen, ist zu schützen. Der DSB kam zum Schluss, dass die Videoüberwachung nicht verhältnismässig ist und forderte die Gemeinde auf, diese anzupassen und die Kameras ausschliesslich ausserhalb der Betriebszeiten des Schwimmbads laufen zu lassen.

§ 8 IDG
Art. 26 Verordnung 3 zum Arbeitsgesetz

04
Umgang mit Verlustscheinen

Eine Gemeinde plante, die Aufarbeitung offener Verlustscheine aus der Alimentenbevorschussung und aus Krankenkassenprämien aus Kapazitätsgründen an eine private Inkassofirma abzutreten. Sie wandte sich daher an den Datenschutzbeauftragten mit der Bitte, den Dienstleistungsvertrag über das Verlustscheinmanagement und die Allgemeinen Geschäftsbedingungen der Inkassofirma auf ihre Vereinbarkeit mit den datenschutzrechtlichen Anforderungen zu prüfen.
Als Erstes stellte sich in diesem Zusammenhang die Frage der Zulässigkeit einer Abtretung von Verlustscheinen an Private aus datenschutzrechtlicher Sicht.
Der Datenschutzbeauftragte stellte fest, dass im Kanton Zürich gesetzliche Grundlagen, welche Gemeinden zur Bekanntgabe von Personendaten im Rahmen von Forderungsabtretungen ermächtigen, fehlen. Verlustscheine dürfen daher nur mit Einwilligung der betroffenen Schuldner, und sofern keine überwiegenden privaten oder öffentlichen Interessen entgegenstehen, abgetreten werden.
Die Bewirtschaftung der Verlustscheine durch eine private Inkassofirma, während die Gemeinde Gläubigerin der Forderungen bleibt, ist im Rahmen einer Auftragsdatenbearbeitung jedoch zulässig. Der Datenschutzbeauftragte forderte die Gemeinde deshalb auf, den Dienstleistungsvertrag entsprechend den Anforderungen an die Auftragsdatenbearbeitung vollständig zu überarbeiten und darin ausdrücklich festzuhalten, dass die Verlustscheine bewirtschaftet und nicht abgetreten werden.

§ 16 und § 17 IDG
§ 6 IDG
§ 25 IDV

05
Besucherverhalten auf Websites

Ein öffentliches Organ wandte sich im Rahmen der Erneuerung seines Webauftritts für die Überprüfung der neuen Datenschutzerklärung an den Datenschutzbeauftragten.
Der Datenschutzbeauftragte begrüsste die weiterhin transparente Information der Nutzerinnen und Nutzer über die Webangebote. Das öffentliche Organ sah neu den Einsatz von Google Analytics zusammen mit «anonymizeIp» vor. Google Analytics ist eine Software, mit welcher das Besucherverhalten, das sogenannte Besuchertracking, auf Websites ausgewertet werden kann. Dabei werden IP-Adressen der Websitebesucher direkt an die Firma Google weitergeleitet. Eine Kontrolle darüber, wie und zu welchem Zweck die IP-Adressen weiterbearbeitet werden, ist für das öffentliche Organ jedoch nicht möglich – es bleibt aber für die Datenbearbeitung verantwortlich, auch wenn die Informationen automatisch an Dritte weitergeleitet werden. Mit «anonymizeIp» sollen alle IP-Adressen anonymisiert werden. Weil die IP-Adressen aber dennoch noch vor der Anonymisierung an Google übermittelt werden und in der Schweiz (anders als beispielsweise in Deutschland) mit der Firma Google keine Einigung auf vertraglicher Ebene für einen datenschutzkonformen Einsatz des Analysetools möglich ist, hat der Datenschutzbeauftragte den Einsatz eines anderen Tools wie beispielsweise PIWIK empfohlen. Wollen kantonale Organe das Verhalten der Besucher ihrer Website erfassen, müssen sie eine Software einsetzen, welche die datenschutzrechtlichen Rahmenbedingungen erfüllen kann.

06
Elektronische Archivierung von Spitalakten

Im Rahmen eines Datenschutzreviews stellte ein Spital Fragen im Zusammenhang mit der elektronischen Archivierung von Akten. Das Spital wollte insbesondere wissen, ob Originalakten nach dem Einscannen im elektronischen Archiv vernichtet werden können und ob es ausreicht, anstelle der Vernichtung dieser Akten lediglich die Zugriffe darauf zu beschränken.
Bei Spitalakten ist zu differenzieren, ob es sich um die Patientendokumentation oder andere Spitalakten wie beispielsweise Personalakten handelt. Je nach anwendbarem Recht können Originalakten, die zur Archivierung eingescannt werden, vernichtet werden, sofern die Integrität der Daten gewährleistet ist. Dies gilt für die gesamte Patientendokumentation, da diese schriftlich oder elektronisch geführt werden kann. Zu berücksichtigen ist, dass nachträgliche Änderungen nachvollziehbar sein müssen. Für die laufende Ablage der Akten ist ein Aufbewahrungskonzept zu erstellen, das den gesetzlich vorgeschriebenen Fristen Rechnung trägt. Werden die Informationen definitiv nicht mehr benötigt respektive ist die Frist von zehn Jahren nach Abschluss der letzten Behandlung abgelaufen und nicht aus einem vom Gesetz festgehaltenen Spezialgrund verlängert worden, sind die Informationen zu vernichten, sofern sie nicht archiviert werden. Verunmöglichen IT-Systeme eine definitive Löschung elektronischer Akten, ist mit dem IT-Provider eine Lösung zu suchen. Im Sinne einer Übergangslösung können die Informationen verschlüsselt gespeichert und die Zugriffe stark eingeschränkt werden.
In diesem Zusammenhang prüfte der Datenschutzbeauftragte ausserdem, ob das Spital ein eigenes Archiv führen darf. Da das Spital keine selbständige Anstalt des öffentlichen Rechts ist, kann es kein eigenes Archiv führen und hat seine Akten dem Staatsarchiv zur Archivierung anzubieten.

§ 5 Abs. 2 und 3 IDG
§ 7 IDG
§ 13 Abs. 2 Gesundheitsgesetz
§ 17 Abs. 2 Patientinnen- und Patientengesetz
§§ 5 Abs. 1, 6 Abs. 1, 7 und 8 Archivgesetz
§ 10 Abs. 1 Archivverordnung

07
Bewirtschaftung von Personaldossiers

Die Teilrevision des Personalgesetzes betreffend die Bearbeitung von Personendaten und Case Management enthält keinen Vorbehalt mehr bezüglich der Bestimmungen über die Archivierung. An einer Veranstaltung des Staatsarchivs zusammen mit dem Personalamt und dem Datenschutzbeauftragten wurden die sich in der Praxis stellenden personal-, datenschutz- und archivrechtlichen Fragen besprochen.
Die Rechtslage zur Führung von Personaldossiers stellt sich wie folgt dar: Das Personaldossier darf jene Angaben enthalten, welche für die Durchführung des Arbeitsverhältnisses geeignet und erforderlich sind. Unterlagen, welche nach Ablauf einer gewissen Zeitdauer oder bei Beendigung des Arbeitsverhältnisses für dieses nicht mehr erforderlich sind, sind folglich aus dem Dossier zu entfernen. Aufgrund des archivrechtlichen Vorbehalts, welcher gemäss Archivgesetz gilt, dürfen ausgesonderte Unterlagen jedoch erst vernichtet werden, wenn das Archiv diese nicht übernimmt. Bis zum Zeit-

punkt des Entscheids des Archivs müssen diese Unterlagen somit aufbewahrt und dem Zugriff durch die zuvor berechtigten Personen entzogen werden.
In der Praxis zeigte sich allerdings, dass die periodische Bereinigung von Personaldossiers unterschiedlich gehandhabt wird. So erhielt das Staatsarchiv teilweise Dossiers zur Übernahme angeboten, welche entweder gar nie bereinigt oder dann so stark ausgedünnt worden waren, dass sie für das Archiv keinen Überlieferungswert mehr besassen. Beides entspricht nicht der geltenden Rechtslage.
Es wurden verschiedene Lösungsansätze in Bezug auf den Umgang mit ausgesonderten Unterlagen diskutiert, doch keiner führte zu einem für alle Beteiligten befriedigenden Resultat.
Die vom Personalamt im Nachgang zur Veranstaltung gewählte Lösung, die ausgesonderten Unterlagen in einem verschlossenen Couvert aufzubewahren, stellt aus datenschutzrechtlicher Sicht keine adäquate Lösung dar. Mit Blick auf das elektronisch geführte Personaldossier könnte jedoch eine technische Lösung angestrebt werden, welche den gesetzeskonformen Umgang mit ausgesonderten Unterlagen erlaubt.

§§ 5 und 8 IDG
§ 34 PG
§§ 21 ff. VVO PG
§ 8 Archivgesetz

08
Elektronische Identitäten im Hochschulbereich

Die Hochschulen planen, neue, einheitliche elektronische Identitätsnachweise einzuführen. Damit sollen die heute heterogenen Lösungen vereinheitlicht und vereinfacht werden. Studentinnen und Studenten sollen so für die Zeit ihrer Hochschulausbildung nur mit einer statt wie heute einer Vielzahl elektronischer Identitäten ausgestattet werden. Mit dieser einen Identität können sie sich dann bei allen an einem solchen Projekt beteiligten Hochschulen anmelden und auch Angebote von Dritten, beispielsweise Bibliotheken, nutzen. Dies unabhängig vom Standort der Hochschule oder der angebotenen Dienste. Die Identität soll für die gesamte Studiendauer und nach Bedarf auch darüber hinaus gelten.
Aufgrund der verschiedenen an einer solchen Lösung beteiligten Akteure (wie Hochschulen, Studentinnen und Studenten, Anbieter von Dienstleistungen, mit der Ausstellung der Identitäten beauftragte Dritte etc.) ist zu Beginn des Projekts zu klären, welche Institution welche Daten zu welchem Zweck bearbeitet. Das in der Folge anwendbare Datenschutzrecht bestimmt sich nach dem für die jeweilige Datenbearbeitung verantwortlichen öffentlichen Organ.
Aufgrund der Komplexität, der unterschiedlichen Rollen und Prozesse der Beteiligten sowie der unterschiedlich anwendbaren Datenschutzbestimmungen können die entsprechenden datenschutzrechtlichen Fragen nur einzelfallbezogen beantwortet werden. Grundsätzlich zur Anwendung kommen jedoch die in der ganzen Schweiz geltenden datenschutzrechtlichen Prinzipien. Das heisst, es braucht für das Bearbeiten der Daten eine Rechtsgrundlage oder einen Rechtfertigungsgrund. Die Daten dürfen nur verhältnismässig und zweckgebunden bearbeitet werden. Sie müssen durch organisatorische und technische Massnahmen geschützt und – sobald sie nicht mehr benötigt werden oder wenn die betroffene Person dies verlangt – gelöscht werden.

09
Forschungsprojekt zur Aufarbeitung der Heimgeschichte

Ein wissenschaftliches Institut führt ein Forschungsprojekt zur Aufarbeitung der Schweizer Heimgeschichte durch. Dabei werden unter anderem Heimakten, welche sich in einem kommunalen Archiv befinden, ausgewertet und es wird nach Zeitdokumenten wie Fotografien recherchiert. Die Ergebnisse sollen veröffentlicht werden. Das Forschungsinstitut wandte sich mit Fragen zur Anonymisierung von Namen ehemaliger Heimleitender und Mitarbeitender sowie zur Verwendung von Fotografien an den Datenschutzbeauftragten.

Bezüglich der Anonymisierung von Namen ist zunächst zu unterscheiden, ob es sich um ein Dokument im Archiv handelt, dessen Schutzfrist abgelaufen ist oder nicht. Während der Schutzfrist kann zu Forschungszwecken Zugang zu archivierten Akten gewährt werden. Dabei dürfen aus den Forschungsresultaten keine Rückschlüsse auf bestimmte Personen möglich sein. Sollen Personen namentlich genannt werden oder ist die Anonymisierung nicht möglich, ist die Publikation nur mit Einwilligung der betroffenen Personen zulässig. Nach Ablauf der Schutzfrist werden die Akten frei zugänglich. Dies befreit jedoch nicht von der Pflicht, den Schutz der Persönlichkeit der betroffenen Personen zu wahren. Lebt die betroffene Person noch, ist aufgrund einer Interessenabwägung zu entscheiden, ob Informationen über ehemalige Heimleitende und Mitarbeitende publiziert werden sollen. Handelt es sich um Darstellungen, welche geeignet sind, die Persönlichkeit der betroffenen Personen zu verletzen, sind diese anonymisiert oder mit Einwilligung der betroffenen Person zu publizieren. Für die Interessenabwägung spielt es eine massgebliche Rolle, in welchem Kontext die betroffene Person erwähnt wird. Das Interesse am Schutz der Persönlichkeit ist gegenüber dem Forschungsinteresse abzuwägen. Letzteres wird aber nur in Ausnahmefällen eine personifizierte Berichterstattung verlangen. Ist die betroffene Person dagegen verstorben, ist die Publikation grundsätzlich zulässig, da der Persönlichkeitsschutz mit dem Tod endet. Ein beschränkter postmortaler Persönlichkeitsschutz besteht im Andenkensschutz von Verstorbenen. Wie weit dieser geht, ist allerdings offen. Auch hier ist zu berücksichtigen, in welchem Kontext die verstorbene Person erwähnt wird sowie wann diese verstorben ist. Mit zunehmendem zeitlichem Abstand zum Todeszeitpunkt ist von einem geringeren Andenkensschutz von Verstorbenen auszugehen.

Bei der Publikation von Fotografien ist massgebend, ob die abgebildeten Personen erkennbar sind. Sind diese erkennbar, bedarf die Publikation der Einwilligung der abgebildeten Personen. Ist eine abgebildete Person verstorben, gelten die obigen Ausführungen zum Andenkensschutz analog.

§ 16 Abs. 1 lit. b IDG
§ 11a lit. c Archivgesetz

10
Gefährdungsmeldungen durch Schulpsychologen

Eine Schulpsychologin gelangte mit der Frage an den Datenschutzbeauftragten, wie sie bei einem konkreten Verdacht auf Kindesmisshandlung vorzugehen habe und ob sie einschlägige Informationen, die durch die Schweigepflicht geschützt sind, an involvierte Stellen weitergeben dürfe.

Bei Verdacht auf Kindesmisshandlung oder generell, wenn

das Wohl einer Schülerin oder eines Schülers gefährdet ist und die Eltern nicht von sich aus für Abhilfe sorgen, informiert die Lehrperson die Schulleitung. Diese informiert die Schulpflege, welche der Kindes- und Erwachsenenschutzbehörde (KESB) eine Gefährdungsmeldung erstatten kann. Diese Meldung kann auch gegen den ausdrücklichen Willen des Kindes und/oder der Eltern erfolgen, da im Falle einer Gefährdung das Kindeswohl höher zu gewichten ist als der Wunsch nach Geheimhaltung. Bleibt die Schule untätig, kann die Lehrperson subsidiär direkt der KESB eine Gefährdungsmeldung erstatten. Auf Gesuch der Schule kann die Schulärztin oder der Schularzt ein Kind auch ohne Zustimmung der Eltern untersuchen und Misshandlungszeichen dokumentieren, die für die KESB wichtig sein können. Wer für die Überweisung an den Schularzt zuständig ist, ist schulintern zu regeln.
Möchte die Schulpsychologin oder der Schulpsychologe ausser der Verdachtsmeldung weitere Informationen mit der Schulärztin oder dem Schularzt austauschen, sollte aufgrund der ungeklärten Rechtslage vorgängig eine Entbindung vom Berufsgeheimnis eingeholt werden. Werden Schulpsychologinnen und -psychologen von der KESB zur Mitwirkung im Kindesschutzverfahren angehalten, sind sie verpflichtet, Bericht zu erstatten und alle für den Fall relevanten Auskünfte zu erteilen. Auch hier sollten sie sich vorgängig vom Berufsgeheimnis entbinden lassen.

Art. 321 Ziff. 1 und 2 StGB
Art. 446 ZGB
Art. 448 Abs. 2, 3 und 4 ZGB
§ 16 und § 17 IDG
§ 51 VSG
§ 16 Abs. 4 VSV

11
Keine sensitiven Schülerdaten auf Lernplattform

Eine heilpädagogische Schule wandte sich an den Datenschutzbeauftragten mit der Frage, ob sensitive Personendaten wie medizinische und schulpsychologische Informationen auf educanet2 gespeichert und bearbeitet werden dürfen. Bei educanet2 handelt es sich um eine für Schulen konzipierte Arbeits- und Lernplattform, die 2001 im Rahmen des Schweizerischen Bildungsservers educa.ch im Auftrag von Kantonen und Bund lanciert wurde.
Die datenschutzrechtlichen Abklärungen ergaben, dass seitens educanet2 die für eine Bearbeitung sensitiver respektive besonderer Personendaten erforderlichen Sicherheitsmassnahmen nicht komplett umgesetzt worden waren. So ist die Verbindung zur Plattform zwar verschlüsselt und Dokumente können auf dieser auch verschlüsselt gespeichert werden. Jedoch fehlt insbesondere eine starke Authentifizierung, die den Schutz vor Zugriffen durch Unberechtigte gewährleistet (sogenannte Zwei-Faktor-Authentifizierung). Da die Vertraulichkeit nicht sichergestellt werden kann, ist die Plattform für eine Bearbeitung besonderer Personendaten nicht geeignet. Der Datenschutzbeauftragte wandte sich diesbezüglich an das Volksschulamt und an educa.ch. Gemäss ihren Antworten wird Schulen empfohlen, educanet2 als reine Arbeits- und Lernplattform zu nutzen, wobei in der Regel keine sensitiven Informationen anfallen. Nach übereinstimmender Ansicht der involvierten Stellen und des Datenschutzbeauftragten sind die Nutzungsbedingungen von educanet2 dahingehend zu ergänzen, dass keine sensitiven Informationen auf der Plattform gespeichert und bearbeitet werden dürfen.

§ 7 IDG

12
Einsichtsrecht in Akten von Drittpersonen

Der Datenschutzbeauftragte hat zu einem Rechtsgutachten Stellung genommen, das sich mit der Frage befasst, ob Verwaltungs- und Gerichtsbehörden berechtigt sind, dem Ombudsmann Auskünfte und Akten gestützt auf das Gesetz über die Information und den Datenschutz (IDG) zu verweigern, wenn sich das Begehren auf Akten Dritter bezieht, die der Ombudsmann für Abklärungen in einem Verfahren für erforderlich hält. Die Autoren des Gutachtens kommen zum Schluss, dass die Verwaltungs- und Gerichtsbehörden verpflichtet seien, der Ombudsperson alle für einen Fall relevanten Akten vorzulegen und die gewünschten Auskünfte zu erteilen. Die Herausgabe von darunter fallenden Akten Dritter könne nicht mit der Begründung verweigert werden, es lägen überwiegende Interessen dieser Dritten vor.

Der Datenschutzbeauftragte hielt in einer Stellungnahme zum Gutachten zunächst fest, dass sich die Aufgaben der Ombudsperson mit den Aufgaben des Datenschutzbeauftragten, der Finanzkontrolle oder einer parlamentarischen Untersuchungskommission vergleichen lassen. Aus der gesetzlichen Aufgabenumschreibung der Ombudsperson kann abgeleitet werden, dass der Ombudsperson Einsicht in Dokumente zu gewähren ist. Die Ombudsperson darf Personendaten bearbeiten, wenn dies zur Erfüllung ihrer Aufgaben geeignet und erforderlich ist. Deshalb dürfen bzw. müssen ihr andere öffentliche Organe Personendaten bekanntgeben. Eine verfahrensrechtliche Bestimmung bezüglich der Ombudsperson regelt zusätzlich ausdrücklich die Erhebungen der Informationen im Verfahren. Darin ist festgehalten, dass die am Verfahren beteiligten Behörden zur Auskunft und Vorlage der Akten an die Ombudsperson verpflichtet sind. Diese Bestimmung stellt keine Amtshilfebestimmung dar, sondern eine Rechtsgrundlage für eine Pflicht zur Datenbekanntgabe.

Weiter hielt der Datenschutzbeauftragte in seiner Stellungnahme fest, dass jede Bekanntgabe von Personendaten unter dem Vorbehalt steht, dass bei einem überwiegenden öffentlichen oder privaten Interesse oder einer entgegenstehenden gesetzlichen Bestimmung keine oder eine eingeschränkte Bekanntgabe zu erfolgen hat. Ein öffentliches Organ hat deshalb bei jeder Datenbekanntgabe eine Interessenabwägung vorzunehmen und zu prüfen, ob entgegenstehende Interessen vorhanden sind. Entgegenstehende Interessen können jedoch nur zu einer Beschränkung oder Verweigerung der Bekanntgabe führen, wenn sie überwiegen. Dies gilt auch für alle Datenbekanntgaben gestützt auf eine Rechtsgrundlage. Folglich kann im Einzelfall – selbst wenn eine Rechtsgrundlage die Bekanntgabe von Informationen erlaubt – die Bekanntgabe eingeschränkt oder verweigert werden. Möchte beispielsweise die Ombudsperson im Rahmen einer Lohngleichheitsfrage Einsicht in ein Personaldossier einer dritten Person nehmen, so ist diese Einsicht nicht für das gesamte Personaldossier zu gewähren, sondern auf die Anstellungsverfügungen dieser dritten Person zu beschränken. Keine Einsicht erhält die Ombudsperson beispielsweise in Arztzeugnisse oder andere für den konkreten Fall nicht relevante Unterlagen, welche sich auch im Personaldossier befinden. Die Interessen der Ombudsperson überwiegen bezüglich der Anstellungsverfügung, nicht jedoch in Hinsicht auf die Arztzeugnisse – hier überwiegen die Interessen der betroffenen Person. Die Interessenabwägung ist Ausfluss des verfassungsmässigen Rechts auf Schutz der Privatsphäre der betroffenen Dritten.

§ 89 VRG
§ 92 VRG
§ 8 IDG
§ 16 und 17 Abs. 1 lit. a IDG
§ 23 IDG

13
Einsatz einer Plagiatserkennungssoftware

Eine Hochschule beabsichtigte, zur Erkennung von Plagiaten in wissenschaftlichen Arbeiten eine neue Software einzusetzen, und wandte sich mit der Frage an den Datenschutzbeauftragten, wie diese Software datenschutzkonform genutzt werden kann.
Es handelt sich dabei um ein Produkt eines Safe-Harbor-zertifizierten US-amerikanischen Unternehmens. Beim konkreten Einsatz gibt die Hochschule die Arbeiten, die sie auf Plagiate überprüfen will, bekannt, ohne sie zu anonymisieren oder zu pseudonymisieren. Diese Arbeiten werden auf der softwareeigenen Datenbank in den USA gespeichert und auch für künftige Plagiatskontrollen verwendet. Der Datenschutzbeauftragte beurteilte die vorgelegten Vertragsbestimmungen sowie die Allgemeinen Geschäftsbedingungen anhand der datenschutzrechtlichen Anforderungen an ein Bearbeiten im Auftrag. Diese Anforderungen richten sich nach Art und Inhalt respektive dem Schutzbedarf der durch die Dritten zu bearbeitenden Daten. Der Datenschutzbeauftragte hielt in seiner Antwort fest, dass zur Transparenz und aufgrund der Verantwortung der Hochschule für ihre Daten der Umgang mit diesen – namentlich die Verantwortung, die Verfügungsmacht, die Zweckbindung und die Bekanntgabe sowie die Geheimhaltung, die Rechte Betroffener, die Kontrolle, Unterauftragsverhältnisse und die Informationssicherheit – vertraglich zu regeln seien. Auch müsse der Ort bekannt sein, an dem die Daten bearbeitet werden. Bei Datenbearbeitungen in Ländern mit keinem der Schweiz angemessenen Datenschutzniveau sind ausserdem zusätzliche rechtliche und technische Massnahmen zu ergreifen wie der Abschluss spezifischer Abkommen oder eine Verschlüsselung.
Bei der konkreten Prüfung stellte der Datenschutzbeauftragte fest, dass die Software durch den Einsatz von Cookies, durch Webtracking und Social-Media-Funktionen Personendaten unkontrolliert weitergibt. Der Datenschutzbeauftragte wird die Hochschule bei der Umsetzung der datenschutzrechtlichen Anforderungen in rechtlicher und technischer Hinsicht unterstützen, um eine datenschutzkonforme Lösung zu finden.

§ 6 IDG
§ 25 IDV
§ 7 IDG

14
Datenaustausch zwischen KESB und Gemeinden

Eine Gemeinde hat sich mit der Frage an den Datenschutzbeauftragten gewandt, wie es sich bezüglich Datenaustausch zwischen dem Sozialamt und der Kinder- und Erwachsenenschutzbehörde (KESB) verhält, wenn die Gemeinde ihre Kostenübernahmepflicht prüfen möchte. Der Datenschutzbeauftragte hat die Gemeinde dahingehend beraten, dass die Schweigepflicht im Kindes- und Erwachsenenschutzrecht als bundesrechtliche Bestimmung den kantonalen Amtshilfebestimmungen des Sozialhilfegesetzes vorgeht und daher keine Rechtsgrundlage für den Austausch besteht. Als Lösungsweg schlug er vor, die Informationen gestützt auf die Einwilligung der betroffenen Person auszutauschen und weitere Abklärungen bezüglich der Frage, welche Kostenträger für eine Massnahme aufkommen müssen, unter Einbezug der Betroffenen zu tätigen.

Diese und ähnliche Fragen stellen sich in der Praxis immer wieder. Die Bestimmungen sowohl des Bundes- wie auch des kantonalen Rechts im Bereich des Kindes- und Erwachsenenschutzes sehen nicht für alle Fragen eine abschliessende Regelung vor. Für die Beantwortung der sich im Zusammenhang mit der Zusammenarbeit (und auch mit dem Informationsaustausch zwischen) der KESB und der Gemeinde stellenden Fragen haben der Verband der Gemeindepräsidenten des Kantons Zürich (GPV), die KESB-Präsidienvereinigung Kanton Zürich (KPV) sowie die Sozialkonferenz Kanton Zürich (SoKo) «Empfehlungen zur Zusammenarbeit zwischen den Gemeinden und den KESB im Kanton Zürich» herausgegeben. Inhalt der Empfehlungen sind Grundsätze zur Zusammenarbeit von KESB und Gemeinde: allgemeine Handlungsgrundsätze, Aufgaben und Rollen von KESB, Gemeinden, Beiständen und Beiständinnen sowie die Qualitätssicherung. Die Publikation definiert Standards zu spezifischen Schnittstellenthemen wie Gefährdungsmeldungen, Mitwirkung der Gemeinden bei der voraussichtlichen Kostenbeteiligung im Kindesschutz, schulisch indizierten Massnahmen, Sofortplatzierungen von Minderjährigen durch die KESB beziehungsweise Notplatzierungen von Minderjährigen durch Dritte, Informationsaustausch, Übernahme von Massnahmen, Entschädigung für die Mandatsführung bei Wohnsitzwechsel sowie Haftung.

Die Empfehlungen heben insbesondere hervor, dass die KESB jeweils im Einzelfall eine Interessenabwägung vornehmen muss, bevor sie Dritten Auskunft erteilen kann. Ihre Schweigepflicht gilt auch gegenüber Gemeinden. Die Durchbrechung dieser Schweigepflicht ist nur zulässig, wenn überwiegende Interessen entgegenstehen. Als mögliche überwiegende Interessen an einer Auskunftserteilung erwähnen die Empfehlungen die Notwendigkeit der Informationsweitergabe durch die KESB zur Wahrnehmung der Interessen der betroffenen Person oder eine ernsthafte Gefährdung der betroffenen Person oder Dritter. Die Empfehlungen umschreiben zudem das Vorgehen bei der Einholung des Amtsberichtes bei der Wohnsitzgemeinde durch die KESB. Demnach nimmt die KESB eine Interessenabwägung vor und prüft auch in diesem Fall, ob die Mitteilung der Verfahrenseröffnung an die Gemeinde verhältnismässig ist. Der Datenschutzbeauftragte hat die Empfehlungen geprüft und erachtet sie als ausgewogen. Sie stellen eine praxisbezogene Handlungsanleitung zur Verfügung.

Art. 451 Abs. 1 ZGB
§ 48 Abs. 2 SHG
§ 49 Abs. 2 EG KESR

Verhandlungen

«Die Kontrolle über die persönlichen Daten wird gestärkt, indem der Zugang zu den eigenen Daten vereinfacht, das Recht auf Vergessen und das Recht auf Portabilität verankert werden.»

Informationsverwaltung und -sicherheit noch nicht am Ziel

Viele Gesetzgebungsvorhaben haben einen Bezug zum Datenschutz, da sie Datenbearbeitungen beinhalten. In den Vernehmlassungsverfahren prüft der DSB, wie die rechtlichen, organisatorischen und technischen Vorgaben des Datenschutzes umgesetzt werden. Er nimmt Stellung zu den relevanten Bestimmungen und macht allenfalls Vorschläge für eine datenschutzkonforme Umsetzung in der Gesetzgebung.

Dabei sind auch viele Gesetzgebungsvorhaben zu prüfen, die sich im Nachhinein als nicht datenschutzrelevant erweisen oder bereits datenschutzkonform ausgestaltet sind, so dass sich eine Stellungnahme erübrigt. Die wichtigen und zeitintensiven Vernehmlassungen werden als Richtgrösse ausgewiesen. Die vorgesehene Anzahl von 18 wurde mit 23 Vernehmlassungen im Jahre 2015 um über einen Viertel überschritten.

Der DSB beurteilt Entwürfe von Erlassen und Vorhaben im Gesetzgebungsverfahren mit Bezug zu Datenschutz und/oder Informationssicherheit. Dazu verfasst er Vernehmlassungsantworten, Stellungnahmen und Mitberichte. Der Leistungsindikator im KEF gibt Auskunft über die eingereichten Vernehmlassungsantworten, Stellungnahmen und Mitberichte.

KEF	18
2015	23

Auf kantonaler Ebene wurde im Bereich der Informationssicherheit in den letzten beiden Jahren eine neue Verordnung erarbeitet. Der DSB war in die Arbeiten einbezogen und hat im Rahmen der Vernehmlassung Stellung genommen. Anlässlich der verwaltungsinternen Konsultation nahm er zum Entwurf einer Informationsverwaltungsverordnung Stellung. Nebst inhaltlichen Bemerkungen waren zentrale Anliegen, dass eine Verordnung (statt bloss verwaltungsinterner Richtlinien) erlassen und der Erlass inhaltlich auf die Informationssicherheitsverordnung abgestimmt wird.

Zu datenschutzrechtlich relevanten Gesetzgebungsvorhaben des Bundes nimmt der Datenschutzbeauftragte Stellung, sofern es sich dabei um sensible Datenbearbeitungen oder um Gesetzgebungsvorhaben von grundlegender Bedeutung für das Datenschutzrecht handelt.

Der DSB kann sich dabei teilweise auf Vernehmlassungen der Vereinigung der schweizerischen Datenschutzbeauftragten – privatim – abstützen, die den Datenschutzbehörden zur Verfügung gestellt werden oder bei deren Erarbeitung er mitwirkt.

Der Datenschutzbeauftragte hat 2015 unter anderem zu folgenden Gesetzgebungsprojekten Stellung genommen:

Kanton

– Informationssicherheitsverordnung (Neuerlass)
– Regelung über die Informationsverwaltung in der kantonalen Verwaltung (Neuerlass)
– Verordnung über die Datenbearbeitung der Direktion der Justiz und des Innern (Neuerlass)
– Taxigesetz (Neuerlass)
– Nachführung Personalverordnung und Vollzugsverordnung zum Personalgesetz
– Änderung EG KVG (Optimierung des Prämienverbilligungssystems)
– Teilrevision Gesundheitsgesetz (Anpassungen an das neue Epidemiengesetz des Bundes)
– Gesetz über die Integrierte Psychiatrie Winterthur – Zürcher Unterland AG (Neuerlass)
– Gesetz über die Psychiatrische Universitätsklinik Zürich (Neuerlass)

Bund

– Totalrevision des Bundesgesetzes über genetische Untersuchungen beim Menschen
– Bundesgesetz über die Aufarbeitung der fürsorgerischen Zwangsmassnahmen und Fremdplatzierungen vor 1981 (Neuerlass)
– Teilrevision Radio- und Fernsehverordnung
– Teilrevision Zivilstandsverordnung und Verordnung über die Gebühren im Zivilstandswesen

Genetische Untersuchungen beim Menschen

Das Bundesgesetz über genetische Untersuchungen beim Menschen soll totalrevidiert werden. Der Datenschutzbeauftragte nahm zu einzelnen Bestimmungen des Vorentwurfs im Rahmen eines Mitberichts Stellung, namentlich zu Fragen der Aufbewahrung und Vernichtung von Proben und genetischen Daten, der Anonymisierung von Proben, der Rechte der betroffenen Person beim Umgang mit Überschussinformationen und der Durchführung genetischer Untersuchungen im Ausland.
Der Vorentwurf sah vor, dass das Bearbeiten genetischer Daten sowohl den Datenschutzbestimmungen des Bundes wie auch denjenigen der Kantone untersteht. Der Datenschutzbeauftragte wies in seiner Stellungnahme darauf hin, dass nicht nur genetische Daten, sondern auch Proben, das heisst das biologische Material, aus welchem genetische Daten gewonnen werden, unter das Datenschutzrecht fallen. Er regte deshalb eine Ergänzung der entsprechenden Bestimmung an. Zudem stellte er fest, dass eine grundsätzliche Regelung betreffend die Aufbewahrung und Vernichtung von Proben und genetischen Daten, insbesondere im medizinischen Bereich, fehlt. Auch in Bezug auf genetische Untersuchungen bei Arbeitsverhältnissen und bei Versicherungsverhältnissen fehlten detaillierte Regelungen zur Aufbewahrung und Vernichtung von Proben und Untersuchungsresultaten.
Die im Vorentwurf verwendete Begriffstrilogie «anonymisiert», «verschlüsselt» und «unverschlüsselt», welche auch im Humanforschungsgesetz verwendet wird, ist nach Ansicht des Datenschutzbeauftragten missverständlich. Denn es handelt sich dabei nicht um eine «Verschlüsselung» (wie etwa die kryptografische Verschlüsselung für eine Datenübermittlung), sondern um die irreversible, reversible oder eben nicht erfolgende Entfernung des Personenbezugs bei Proben und genetischen Daten. Zutreffender wäre deshalb die Verwendung der Begriffe «anonymisiert», «pseudonymisiert» und «identifizierend». Anonymisierung bedeutet dabei die irreversible Aufhebung des Personenbezugs, so dass Rückschlüsse auf die Person ohne unverhältnismässigen Aufwand nicht mehr möglich sind. Diese Aufhebung des Personenbezugs ist bei Proben menschlicher Körpersubstanzen jedoch nicht möglich, da sie im Rahmen genetischer Analysen jederzeit eindeutig einer Person zugeordnet werden können. Möglich ist einzig, die Informationen zu Proben oder Teilen davon zu entfernen, so dass sich daraus nicht mehr eruieren lässt, von wem das Material stammt. Je mehr biologisches Material erhoben und nicht anonymisiert wird (beispielsweise in populationsbezogenen Biobanken, die mit Material in identifizierender oder höchstens pseudonymisierter Form arbeiten) und je effizienter die einsetzbaren IT-Anwendungen werden, umso kleiner wird der Aufwand zur Zusammenführung und umso höher die Wahrscheinlichkeit, dass durch die Kombinationen von Informationen die Identifizierung der betroffenen Personen dennoch möglich ist. Der Datenschutzbeauftragte empfahl deshalb, bereits heute davon auszugehen, dass biologisches Material auf Dauer nicht wirksam anonymisiert werden kann.
Bei genetischen Untersuchungen können Überschussinformationen anfallen, das heisst Informationen, die für den Zweck der Untersuchung nicht benötigt werden. Die betroffene Person soll gemäss dem Vorentwurf selber entscheiden können, welche Überschussinformationen ihr mitgeteilt werden. Um eine solche Entscheidung treffen zu können, muss sie jedoch darüber aufgeklärt werden, welche Art von Überschussinformationen überhaupt anfallen können. Zudem soll sie auch darüber entscheiden können, zu welchem Zeitpunkt ihr die Überschussinformationen mitgeteilt werden. Der Daten-

schutzbeauftragte schlug vor, die Regelung entsprechend zu ergänzen.
Genetische Untersuchungen sollen unter gewissen Voraussetzungen im Ausland durchgeführt werden können. Als weitere im Gesetzestext zu erwähnende Voraussetzung bedarf es der Gewährleistung eines der Schweiz entsprechenden Datenschutzniveaus. Wenn nicht die Gesetzgebung einen angemessenen Schutz bietet, muss durch andere Massnahmen im Sinne des Bundesgesetzes über den Datenschutz verhindert werden, dass die Persönlichkeit der betroffenen Personen schwerwiegend verletzt wird. Der Datenschutzbeauftragte empfahl eine entsprechende Ergänzung der Bestimmung.

Änderung der Zivilstandsverordnung

Der Datenschutzbeauftragte nahm im Mitberichtsverfahren zu Bestimmungen in der Vernehmlassung zur Revision der Zivilstandsverordnung und der Verordnung über die Gebühren im Zivilstandswesen Stellung.
Die Vorlage sah den Erlass einer neuen Bestimmung vor, wonach aus der Zivilstandsdatenbank Infostar zu allen Änderungen, die Daten aus der Verordnung über das automatisierte Polizeifahndungssystem (RIPOL) betreffen, ein Hinweis an RIPOL übermittelt wird. Dies impliziert, dass die Datenbank Infostar registriert, welche Personenstandsdaten in der Datenbank RIPOL erfasst sind. Der Datenschutzbeauftragte wies darauf hin, dass hierfür keine Rechtsgrundlage besteht und solche Einträge nicht gesetzeskonform wären. Sind keine solchen Einträge vorhanden, müsste die Datenbank Infostar RIPOL bei sämtlichen Änderungen von Personenstandsdaten, auf welche das Bundesamt für Polizei Zugriff hat, einen elektronischen Hinweis übermitteln, also auch betreffend Personen, die gar nicht in RIPOL erfasst sind. Dies verstösst gegen das Verhältnismässigkeitsprinzip. Die Bestimmung ist also in beiden Fällen ungenügend. Aus den Erläuterungen zur Vorlage ergab sich sodann, dass mit der Bestimmung offenbar eine bereits etablierte Praxis gesetzlich geregelt werden sollte, die unverhältnismässig ist. Um sicherzustellen, dass diejenigen Stellen auf Infostar-Daten zugreifen können, die auch dazu berechtigt sind, die Identität einer Person zu überprüfen, reicht das Zugriffsrecht im Abrufverfahren. Der Datenschutzbeauftragte verlangte deshalb die Streichung der neuen Bestimmung.
Des Weiteren schlug der Vernehmlassungsentwurf vor, dass die Bestimmung zur Veröffentlichung von Zivilstandsfällen gestrichen werden soll, was der Datenschutzbeauftragte begrüsste. Die Publikation von Personenstandsdaten erfolgt heute vielfach auch im Internet. Angesichts der technischen Möglichkeiten der Weiterverwendung dieser Daten und der Verknüpfung mit weiteren Personendaten besteht eine erhöhte Gefahr für Persönlichkeitsverletzungen. Die Veröffentlichung von Zivilstandsfällen entspricht daher keinem überwiegenden öffentlichen Interesse mehr.

Neue Informationssicherheitsverordnung

Eine Arbeitsgruppe, bestehend aus Fachleuten aus Gemeinden, Spitälern, der Universität und Fachhochschulen sowie Gerichten, des Datenschutzbeauftragten, der Finanzkontrolle und des Kantonalen IT-Teams (KITT) hat einen Entwurf für eine neue Informationssicherheitsverordnung (ISV) erarbeitet. Hauptpunkte der Revision sind die klare Regelung der Pflichten des Leistungsbezügers und -erbringers, namentlich das Risikomanagement, die Schutzstufen und die Massnahmen, aber auch Aspekte der Sicherheitsorganisation sowie der Klassierung und der Ablage. Die Informatiksicherheitsverordnung aus dem Jahr 1997 ist veraltet und basiert auf dem alten Datenschutzgesetz (DSG). Der Geltungsbereich ist eingeschränkt und die Bestimmungen bezüglich Sicherheitsstufen, Schutzzielen und Massnahmen sind rudimentär. Auch enthält die alte Verordnung praktisch keine Bestimmungen zur Sicherheitsorganisation. Diese Faktoren sowie die rasante technologische Entwicklung und die damit steigenden Anforderungen an die Informationssicherheit waren Anlass für eine komplette Überarbeitung der Verordnung.

Neu soll die ISV für alle öffentlichen Organe im Kanton Zürich gelten. Dies vereinfacht das Bestimmen und Umsetzen der Massnahmen, da derselbe Standard für alle datenbearbeitenden öffentlichen Organe zur Anwendung kommt. Neu werden die Verantwortung, die Aufgaben und die Vorgehensweisen klar bestimmt und umschrieben. So sind die Pflichten des Leistungsbezügers wie auch des Leistungserbringers explizit in der ISV benannt und auch das Vorgehen zur Schutzbedarfsermittlung ist darin festgehalten, wobei neu zwischen zwei statt wie bisher drei Schutzstufen unterschieden wird. Vorsorgemassnahmen für Krisen- und Notfälle werden ebenfalls vorgeschrieben. Auch organisatorische Massnahmen wie das Einsetzen einer oder eines Beauftragten für Informationssicherheit sind klar geregelt. Die Grundlagen orientieren sich an den international geltenden Standards.
Im Entwurf der neuen ISV finden sich auch einzelne Bestimmungen, die sich nicht auf die Informatikmittel sondern auf Aspekte der Informationsverwaltung beziehen. So wird zwischen geschäftlichen und privaten Informationen differenziert und der Umgang ist jeweils unterschiedlich geregelt. Ausserdem enthält der Entwurf Bestimmungen zur Sicherheit der ruhenden Ablage sowie zur Löschung und Vernichtung von darin abgelegten Dokumenten.
Wann und mit welchem Inhalt die neue ISV in Kraft treten wird, lässt sich zurzeit noch nicht abschätzen. Im Rahmen der Vernehmlassung hat sich gezeigt, dass bezüglich einiger Projekte der Informationsverwaltung und der Informationssicherheit Koordinationsbedarf besteht.

Regelungen zur Informationsverwaltung

Der DSB nahm Stellung zum Entwurf einer neuen Regelung zur Informationsverwaltung in der kantonalen Verwaltung, welche im Frühling 2015 in die Vernehmlassung geschickt wurde. Diese legt den korrekten und effizienten Umgang mit Informationen von deren Entstehung bis zum Angebot an das Staatsarchiv fest.
Es sollen transparente und nachvollziehbare Geschäftsabläufe gefördert, die Steuerung der Geschäftsprozesse gestärkt sowie die orts- und personenunabhängige Verfügbarkeit von Unterlagen sichergestellt werden.
Der Datenschutzbeauftragte wies zunächst auf den Regelungsauftrag an den Regierungsrat im IDG hin, für die kantonale Verwaltung das Nähere bezüglich Informationsverwaltung in einer Verordnung zu regeln. Dabei ist zu prüfen, was unter dem Begriff «kantonale Verwaltung» zu subsumieren ist. Denn nicht alle öffentlichen Organe müssen ihre Akten nach Ablauf der Aufbewahrungsfrist dem Staatsarchiv anbieten, sondern können eigene Archive führen.
In Bezug auf den Lebenszyklus der Unterlagen wies der Datenschutzbeauftragte darauf hin, dass die Begriffe mit der neuen Verordnung über die Informationssicherheit abgestimmt werden müssen. Im Rahmen des Vernehmlassungsverfahrens wurde zudem um Stellungnahme zu weiteren Themen gebeten.
Der Datenschutzbeauftragte hielt zur Klassierung von Unterlagen fest, dass sich die Frage stellt, ob eine solche überhaupt notwendig ist. Da vor der Bekanntgabe von Informationen eine Interessenabwägung vorzunehmen ist oder eine Bekanntgabe gestützt auf eine gesetzliche Grundlage erfolgt, ist der Schutz der Informationen auch ohne Klassierung gewährleistet. Zum «Ersetzenden Scanning» (Digitalisierung von eingehender Papierpost mittels Scanning und Bearbeitung nur noch der elektronischen Dokumente ohne parallele Ablage von Papierdokumenten) blieben im Entwurf noch Fragen offen – wie beispielsweise bezüglich der Authentizität der Dokumente, des Umgangs mit Originalunterschriften oder des Eigentums an den Unterlagen. Hinsichtlich von Form und Ebene der Regelung hielt der Datenschutzbeauftragte in seiner Stellungnahme fest, dass nur eine Verordnung dem Geltungsbereich sowie der Tragweite der Regelung Rechnung trägt.

§ 5 Abs. 4 IDG

Neue Datenschutzgesetzgebung in Europa

Die Europäische Union (EU) verabschiedete zwei neue Rechtsakte, die den Datenschutz betreffen: Die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) sowie die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder zum Zweck der Strafvollstreckung sowie zum freien Datenverkehr.

Die neue Datenschutzgesetzgebung wartet mit wesentlichen Neuerungen auf. So ist die Verordnung direkt anwendbar, was eine Harmonisierung des Datenschutzrechts innerhalb der Europäischen Union zur Folge haben wird, da in allen EU-Ländern dieselben datenschutzrechtlichen Standards gelten werden. Ausserdem wird die Kontrolle über die persönlichen Daten gestärkt, indem der Zugang zu den eigenen Daten vereinfacht sowie das Recht auf Vergessen und das Recht auf Portabilität verankert werden. Auch spezielle Regeln für Minderjährige sind darin vorgesehen.

Für Unternehmen gilt, dass sie das EU-Datenschutzrecht berücksichtigen müssen, falls sie Dienstleistungen innerhalb der Europäischen Union erbringen wollen, wenn der Sitz ausserhalb der EU liegt. Nicht zu vernachlässigen sind dabei die Sanktionsmöglichkeiten, die sich am Jahresumsatz der betroffenen Organisationen orientieren.

Die Richtlinie, die Bestimmungen zu den Datenbearbeitungen im Polizei- und Justizbereich enthält, gilt neu nicht nur für den grenzüberschreitenden Datenverkehr, sondern auch für die innerstaatliche Datenbearbeitung. Auch hier werden die Rechte der Betroffenen gestärkt und neue Pflichten verankert, beispielsweise bezüglich der Protokollierung.

Parallel zu diesen Datenschutzerlassen wird auch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates (Übereinkommen 108) einer Revision unterzogen. Es sollten sich keine Widersprüche zu den EU-Erlassen ergeben.

Alle drei Erlasse werden Auswirkungen auf die kantonalen Datenschutzgesetze haben: die Datenschutz-Grundverordnung aufgrund der Tatsache, dass die Datenbearbeitungen vielfach grenzüberschreitenden Charakter haben, und die Richtlinie, da die Schweiz Teil des Schengenraums ist. Bezüglich des Übereinkommens 108 plant der Bund, dieses zu ratifizieren und umzusetzen. Der Datenschutzbeauftragte wird diese Entwicklungen verfolgen und die Umsetzung im Kanton Zürich unterstützen.

«Spitäler bearbeiten grosse Mengen sensitiver Gesundheitsdaten. Kontrollen zeigen, dass grosse Diskrepanzen zwischen erforderlichen und umgesetzten Schutzmassnahmen bestehen.»

Zunehmende Risiken bei der Informationssicherheit

Die Kontrolle und Überprüfung der Datenbearbeitungen der öffentlichen Organe ist ein Schwerpunkt der Tätigkeiten des Datenschutzbeauftragten. Sie umfasst dabei rechtliche, organisatorische und technische Aspekte des Datenschutzes. Neben standardisierten Prüfungen im Rahmen von sogenannten «Datenschutz-Reviews» erfolgen vertiefte Prüfungen und technische Kontrollen. Ebenso sind Kontrollen bei konkretem Anlass vorgesehen.

Als Richtgrösse für das Jahr 2015 waren 40 Kontrollen vorgesehen. Dank der Standardisierung bedeutet dies eine Verdoppelung gegenüber dem Vorjahr. Mit 35 Kontrollen wurde die Zielvorgabe nur leicht unterschritten.

Der DSB kontrolliert die Anwendung der rechtlichen, technischen und organisatorischen Vorschriften über den Datenschutz und die Informationssicherheit durch die öffentlichen Organe. Dazu führt er Datenschutz-Reviews, Kontrollen auf Anlass sowie technische Kontrollen durch. Der Leistungsindikator im KEF gibt Auskunft über die realisierten Kontrollen.

KEF	40
2015	35

Schwerpunktmässig lagen die Kontrollen in den Bereichen Gesundheitswesen, Schulen und Polizei. Im Rahmen eines Pilotprojektes wurde erstmals ein Klinikinformationssystem (KIS) kontrolliert. Breitflächig wurde der Stand der Umsetzung der Informationssicherheit bei den Volksschulen initiiert. Parallel dazu wurden die Kontrollen der Schulwebsites mittels Webscans weitergeführt. Eine Schwerpunktkontrolle galt der Nachführung des Polizei-Informationssystems (POLIS), welche dem DSB als gesetzliche Aufgabe übertragen und erstmals durchgeführt wurde.

Alle Kontrollen zeigten im Ergebnis, dass trotz der Bemühungen der öffentlichen Organe vielfach grundlegende Sicherheitsmassnahmen nicht umgesetzt werden. Im Wissen um die zunehmenden Risiken im Bereich der Informatik durch Angriffe aller Art setzt der Datenschutzbeauftragte in seinen Prüfungen und Kontrollen insbesondere auf die durchgängige Umsetzung der Grundschutzmassnahmen in der Informationssicherheit.

Das Bewusstsein, dass mit dem Umsetzen dieser Grundschutzmassnahmen bereits viel erreicht werden kann, fehlt aber insbesondere bei kleinen Organisationseinheiten oftmals. Zusätzliche Massnahmen sind notwendig, wenn besondere Personendaten bearbeitet werden oder Datenbearbeitungen ausgelagert werden.

Informationssicherheit in den Spitälern

Die Spitäler bearbeiten grosse Mengen sensitiver Gesundheitsdaten. Die Kontrollen haben gezeigt, dass eine grosse Diskrepanz zwischen den erforderlichen und den umgesetzten Schutzmassnahmen besteht. Um den Datenschutz zu verbessern, wird der DSB weitere Kontrollen durchführen.

Bei Gesundheitsdaten bestehen besondere Risiken für Persönlichkeitsverletzungen. Aus diesem Grund überprüfte der Datenschutzbeauftragte im Berichtsjahr die Informationssicherheit in Spitälern. Dabei wurden rechtliche, organisatorische und technische Aspekte mittels einer Schwachstellenanalyse überprüft.

Der hohe Schutzbedarf der Daten von Patientinnen und Patienten erfordert umfangreiche Sicherheitsmassnahmen. In den geprüften Spitälern waren viele dieser Massnahmen inexistent. Dementsprechend fehlten organisatorische Massnahmen wie beispielsweise ein Informationssicherheits- (ISMS) respektive ein Datenschutzmanagementsystem (DSMS) und die darin enthaltenen Elemente wie die Definition von Verantwortlichkeiten, Datenklassifizierung, Massnahmenpläne sowie regelmässige Überprüfungen der Informationssicherheit. Um einen angemessenen und nachhaltigen Schutz zu gewährleisten, ist bei der Bearbeitung von Gesundheitsdaten ein ISMS oder DSMS unabdingbar.

Ferner wurden die technischen Massnahmen in den Bereichen Passwörter, Verschlüsselung und Verwaltung mobiler Geräte (Smartphones, Tablets etc.) ungenügend umgesetzt. Beispielsweise ist bei der Bearbeitung besonderer Personendaten der Einsatz eines Mobile Device Management Systems (MDMS) zwingend erforderlich, insbesondere wenn private Geräte zur Datenbearbeitung genutzt werden (Bring Your Own Device). Ansonsten kann die Verantwortung gemäss dem Gesetz über die Information und den Datenschutz (IDG) nicht wahrgenommen werden.

Der DSB erlangte mit den Kontrollen einen umfassenden Einblick in die Datenbearbeitung eines Spitals und konnte damit die vertieften Kontrollen der Klinikinformationssysteme planen. Er wird weitere Kontrollen und Beratungsdienstleistungen in den Spitälern durchführen, um die datenschutzkonforme Bearbeitung von Gesundheitsdaten zu verbessern.

Kontrolle Klinikinformationssysteme

2015 startete der DSB ein Projekt zur datenschutzrechtlichen Kontrolle von Klinikinformationssystemen (KIS). Das KIS ist die zentrale Informationsplattform des Spitals und aus datenschutzrechtlicher Sicht die sensitivste Applikation. In ihr wird ein Grossteil der Gesundheitsdaten abgelegt. Das Projekt wurde in Zusammenarbeit mit einem grossen Spital durchgeführt.

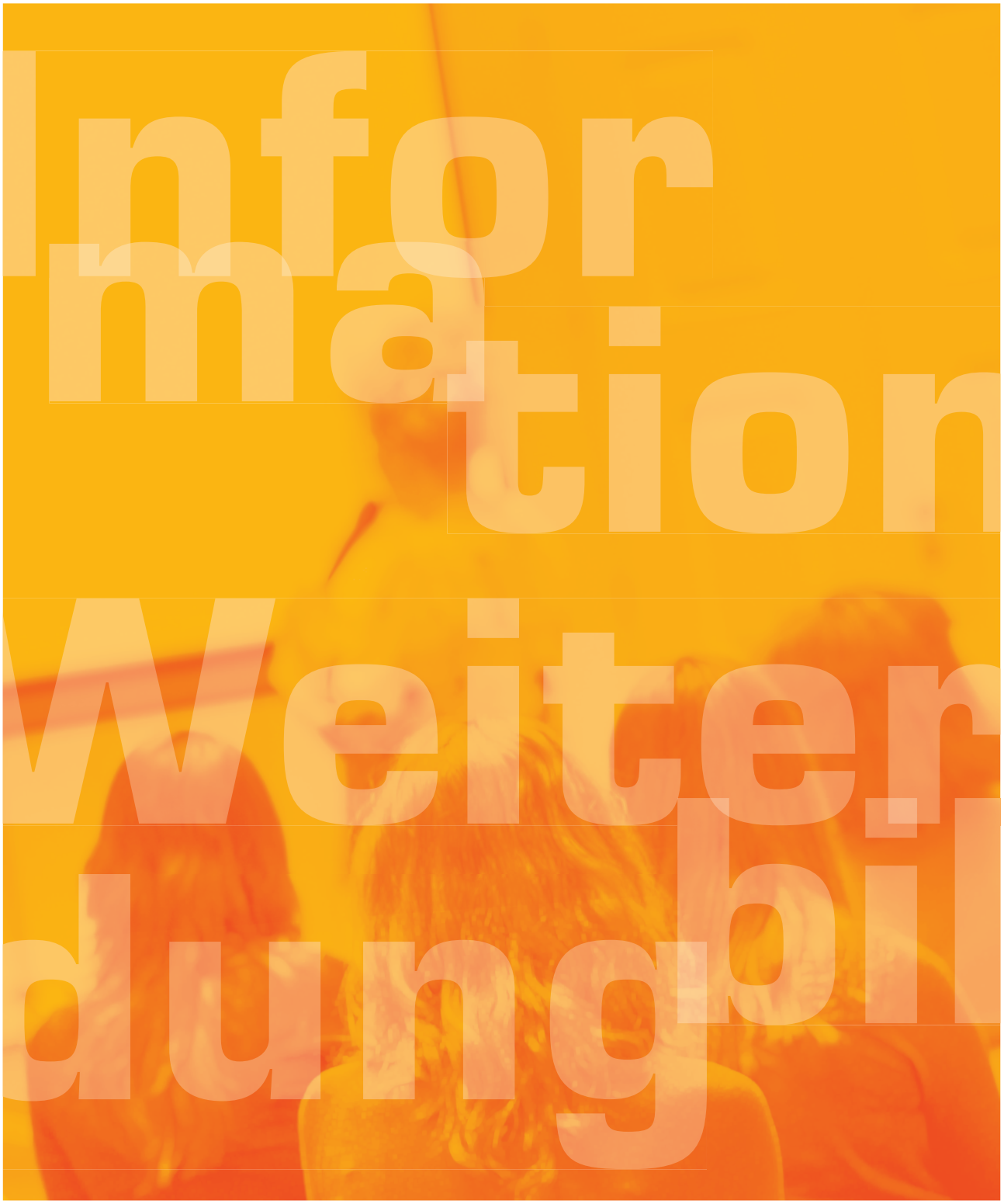
Inhalt der Kontrolle waren einerseits rechtliche Aspekte, wie beispielsweise die Verhältnismässigkeit der Zugriffe, die Umsetzung der Betroffenenrechte, die Archivierung und die Löschung von Personendaten sowie die rechtskonforme Auslagerung der Datenbearbeitungen. Zusätzlich wurden die organisatorischen und technischen Sicherheitsmassnahmen kontrolliert.

So wurde beispielsweise geprüft, ob die Zielsetzungen und Verantwortlichkeiten klar geregelt sind und die Gesundheitsdaten mit angemessenen Massnahmen geschützt werden.
Die Kontrolle zeigte, dass bei der Datenbearbeitung im KIS zahlreiche Schwachstellen bestehen. Beispielsweise wurden die Zugriffe zu wenig eingeschränkt, die Aufbewahrungsfristen nicht mit Blick auf die Gesetzgebung definiert, und es fehlte eine detaillierte Risikoanalyse mit entsprechenden Massnahmenplänen. Anderseits war der organisatorische Überbau mit den entsprechenden Zielsetzungen und Verantwortlichkeiten im geprüften Spital vorbildlich festgelegt.
Um die Resultate breiter abzustützen und daraus Massnahmen zur Verbesserung des Datenschutzes in Spitälern abzuleiten, wird der DSB weitere KIS-Kontrollen durchführen.

Nachführung polizeilicher Datenbearbeitungssysteme

Am 1. März 2013 ist das teilrevidierte Polizeigesetz in Kraft getreten. Dieses verpflichtet den Datenschutzbeauftragen, die Aktualität und die Nachführung der im Polizei-Informationssystem (POLIS) gespeicherten Daten alle zwei Jahre oder aus besonderem Anlass zu kontrollieren.
Die Applikation POLIS wird von der Kantonspolizei Zürich (KAPO), der Stadtpolizei Zürich, der Stadtpolizei Winterthur sowie den kommunalen Polizeien des Kantons Zürich als Datenbearbeitungs- und Informationssystem eingesetzt. Die Nachführung der darin gespeicherten besonderen Personendaten erfolgt unter anderem aufgrund der von den Strafbehörden im Rahmen des gesetzlichen Auftrags innert 14 Tagen nach Eintritt der Rechtskraft mitgeteilten Freisprüche, Einstellungen und Nichtanhandnahmen von Strafverfahren.
Die Hauptverantwortung für die Datenhaltung und -pflege sowie für den Schutz und die Sicherheit der gespeicherten Daten trägt die Kantonspolizei.
Die gesetzlich vorgeschriebene datenschutzrechtliche Kontrolle wurde 2015 erstmalig durchgeführt. Der Fokus der Prüfung lag auf dem KAPO-internen Prozess «Nachführung der polizeilichen Datenbearbeitungssysteme» sowie auf der Informationssicherheit der Applikation POLIS.
Im Rahmen der durchgeführten Kontrolle wurden keine wesentlichen Defizite festgestellt.

§ 54 lit. a PolG



«Durch die Zusammenarbeit mit einer Fachhochschule können die Zielgruppen besser erreicht und die Attraktivität der Angebote gesteigert werden.»

Kontinuierliche Weiterbildung

Das Informations- und Weiterbildungsangebot des Datenschutzbeauftragten ist vielfältig. Es richtet sich nach den Bedürfnissen der verschiedenen Zielgruppen. Neben einem breiten Informationsangebot auf der Website gehören dazu Referate und Veranstaltungen. Des Weiteren haben die Sozialen Medien eine zunehmende Bedeutung. Neben diesen Informationsangeboten bietet der Datenschutzbeauftragte auch gezielte Aus- und Weiterbildungen im Bereich des Datenschutzes an.

Der DSB bietet Aus- und Weiterbildungen im Bereich des Datenschutzes und der Informationssicherheit an. Dies erfolgt in der Form von internen oder externen Seminaren, Kursen, Workshops, Web-Trainingsprogrammen und Referaten. Der Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote für öffentliche Organe.

KEF	20
2015	17

Aufgrund der beschränkten Ressourcen ist das Aus- und Weiterbildungsangebot für öffentliche Organe auf 20 Halbtage beschränkt. Im Jahre 2015 konnten 17 Angebote realisiert werden. Ausbildungsangebote in Form von fachspezifischen Referaten werden dabei nicht mitgezählt.

Die Nachfrage nach Aus- und Weiterbildungsangeboten im Bereich Datenschutz nimmt seit Jahren zu. Neben Grundlagenkursen werden vermehrt Seminare für bestimmte Themenbereiche gewünscht. Um diese Nachfrage besser koordinieren und die Zielgruppen breiter erreichen zu können, hat der Datenschutzbeauftragte eine Kooperation mit der ZHAW aufgebaut. Im Rahmen des ITPZ (Zürcher Zentrum für Informationstechnologie und Datenschutz) soll ein attraktives und nachhaltiges Ausbildungsangebot entstehen, ohne die Ressourcen des Datenschutzbeauftragten zusätzlich zu belasten. Damit können die Kursteilnehmenden von den Vorteilen einer Fachhochschule profitieren und Datenschutzkurse in ihr kontinuierliches Weiterbildungscurriculum integrieren.

Mit bereichsspezifischen Ausbildungsangeboten – beispielsweise im Gesundheits- oder Sozialbereich – werden zudem gezielter die praktischen Fragestellungen der Teilnehmenden aufgegriffen. Die Feedbacks aus den bisherigen Kursen waren durchwegs positiv.

Seminarangebot mit neuer Trägerschaft

Die Zusammenarbeit mit der Zürcher Hochschule für Angewandte Wissenschaften (ZAHW) in der Aus- und Weiterbildung konnte institutionalisiert werden. Im Berichtsjahr wurde das Aus- und Weiterbildungsangebot auf eine neue Trägerschaft gestellt (siehe Tätigkeitsbericht 2014, Seite 38). Die DSB-Seminare Datenschutz im Sozialbereich sowie Datenschutz im Gesundheitswesen werden neu in Zusammenarbeit mit der ZHAW und dem Verein Zürcher Zentrum für Informationstechnologien und Datenschutz (ITPZ) durchgeführt. Mit der ZHAW wurde eine entsprechende Vereinbarung abgeschlossen. Durch die Zusammenarbeit mit der Fachhochschule können die Zielgruppen besser erreicht und die Attraktivität der Angebote gesteigert werden. Das Seminarangebot wird laufend erweitert.

Gemeindefachschule

Im Auftrag des Vereins Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV) hat die KV Business School einen neuen Lehrgang entwickelt, der 2016 erstmals durchgeführt wird. Die neue «Gemeindefachschule» richtet sich an ambitionierte kaufmännische Mitarbeitende aus der öffentlichen Verwaltung, die sich für ihre berufliche Entwicklung bei einer Gemeindeverwaltung oder in verwaltungsnahen Betrieben ein breites Know-how sowie erste Spezialisierungen erwerben wollen. Sie kann mit dem kantonalen Fachausweis Gemeindefachfrau/Gemeindefachmann oder mit dem eidgenössischen Fachausweis Fachfrau/Fachmann öffentliche Verwaltung abgeschlossen werden. Der Datenschutzbeauftragte ist im Fach «Informationssicherheit/Datenschutz» beteiligt.

Seminare und Kursmodule

- Seminar Datenschutz im Sozialbereich
- Seminar Datenschutz im Gesundheitswesen
- Seminar Datenschutz – Vertiefung für Juristinnen und Juristen
- CAS «Clinical Trial Management» (Universität/Universitätsspital)
- CAS Kindes- und Erwachsenenschutzrecht (ZHAW)
- Gemeindefachschule (KV Business School)

Ausgewählte Referate

- Cloud und Datenschutz
- Selbstbestimmt oder fremdbestimmt? Der Schutz der Privatsphäre ist keine private Angelegenheit
- IT-Strategien und Datenschutz: In die «Cloud», aber sicher!
- Datensicherheit im Gesundheitswesen
- Transparenter Staat oder transparenter Bürger?

Informationssicherheit im Fokus

Das Thema Informationssicherheit stand im Mittelpunkt der Kommunikationsaktivitäten des Datenschutzbeauftragten. Zudem erreichte der DSB zum vierten Mal in Folge erfolgreich die Rezertifizierung nach der ISO-Norm 9001.
Die rasante technologische Entwicklung bestimmte thematisch die Kommunikationstätigkeit des Datenschutzbeauftragten im Jahre 2015: Zwei Merkblätter sowie zwei Checklisten wurden veröffentlicht, die sich der Informationssicherheit widmen. Es handelt sich um die Checklisten bezüglich der Datenschutzeinstellungen bei Windows 10 und der Verhinderung von Webtracking. Sie geben den Userinnen und Usern wertvolle Tipps, wie sie vermeiden können, dass bei der Nutzung gewisser Online-Dienste ungewollt Daten über sie gesammelt werden. Das Merkblatt «Online-Speicherdienste» enthält neben einer Aufklärung über die generellen Risiken solcher Dienste auch einen Vergleich gängiger Anbieter bezüglich wichtiger Datenschutzkriterien. Und das Merkblatt «Selbstdatenschutz – sichere E-Mails» thematisiert die drei wichtigsten Massnahmen für die sichere Nutzung von E-Mails – risikoarmes Verhalten, Vertraulichkeit sowie die strikte Umsetzung technischer Schutzmassnahmen.

Wie in den Vorjahren beantwortete der Datenschutzbeauftragte eine grosse Anzahl Anfragen von Medienschaffenden. Hier stand das Thema Informationssicherheit ebenfalls im Zentrum des Interesses, sei es bei Fragen rund um die Risiken der Nutzung Sozialer Medien sowie des Einsatzes mobiler Geräte wie Smartphones und Tablets oder bei der Thematik der immer engmaschiger werdenden Überwachung des öffentlichen Raums.

Ein wichtiger Meilenstein war im Mai 2015 die erfolgreiche vierte Rezertifizierung des Qualitätsmanagementsystems des Datenschutzbeauftragten nach der ISO-Norm 9001. Das Qualitätsmanagementsystem unterstützt den DSB bei der Erfüllung seiner gesetzlichen Aufgaben und garantiert eine wirkungsorientierte und kundenfreundliche Beratungs-, Informations- und Kontrolltätigkeit. Der DSB verfügt seit 2003 über ein zertifiziertes Qualitätsmanagementsystem und gehört damit bei der öffentlichen Hand zu den Pionieren.

Jubiläumssymposium

Bereits zum 20. Mal fand Ende August 2015 das Symposium on Privacy and Security der Stiftung für Datenschutz und Informationssicherheit statt. Ob die unkontrollierte Datensammlung und -verwertung und die damit verbundene Kommerzialisierung vieler Lebensbereiche eine Gefahr für das Fundament unserer demokratischen Gesellschaft darstellen, war dabei eine der wichtigsten debattierten Fragen.

Ausblick

«Die Datenschutzreformen auf europäischer und eidgenössischer Ebene werden auch die Weiterentwicklung des Informations- und Datenschutzgesetzes (IDG) beeinflussen.»

Stärkung des Datenschutzes

In Europa und in der Schweiz sind Datenschutzreformen im Gange, die auch das Informations- und Datenschutzgesetz (IDG) betreffen. In naher Zukunft wird sich der Reformbedarf im Einzelnen konkretisieren.

Die rasante Entwicklung der Informationstechnologie bringt immer wieder neue Möglichkeiten der Datenbearbeitungen, die auch zunehmende Risiken für die persönliche Freiheit und die Privatsphäre beinhalten. Um diesen Herausforderungen der Informations- und Kommunikationsgesellschaft gerecht werden zu können, hat die Europäische Union (EU) ein neues Datenschutzregime verabschiedet, das voraussichtlich 2018 in Kraft treten wird. Es besteht aus einer neuen allgemeinen Grundverordnung und einer Richtlinie für den Polizei- und Justizbereich.

Auswirkungen auf die Schweiz

Es ist davon auszugehen, dass Bund und Kantone nicht um eine Übernahme dieser Weiterentwicklungen herumkommen werden – aufgrund der Schengen-Relevanz der neuen Richtlinie und wegen der Voraussetzung des angemessenen Datenschutzniveaus für einen ungehinderten Datentransfer zwischen den EU-Staaten und der Schweiz. Die Richtlinie ist klar Schengen-relevant. Falls nicht das Risiko eingegangen werden soll, dass die Schengen-Assoziierung der Schweiz aufgelöst wird, wird die Schweiz die Richtlinie übernehmen müssen. Sie betrifft nicht nur den Datenaustausch mit den EU-Staaten, sondern gilt auch für den innerstaatlichen Bereich von Polizei und Justiz. Obwohl die Grundverordnung nicht Schengen-relevant ist, ist sie trotzdem nicht bedeutungslos für die Schweiz. Sie hält nämlich auch fest, dass eine Übermittlung personenbezogener Daten an ein Drittland (wie die Schweiz) nur erfolgen darf, wenn die EU-Kommission festgestellt hat, dass das betreffende Drittland ein angemessenes Schutzniveau bietet. Die öffentliche Verwaltung wie auch die Wirtschaft haben ein erhebliches Interesse daran, dass die EU-Kommission das in der Schweiz gebotene Schutzniveau als angemessen beurteilt.

Des Weiteren ist eine Revision der Europarats-Konvention 108 im Gange, die direkten Einfluss auf das Datenschutzrecht in Bund und Kantonen haben wird. Die Konvention stellt eine Art Minimalstandard im globalen Datenaustausch dar.

Revision des DSG

Bereits hat der Bundesrat eine Revision des Datenschutzgesetzes (DSG) angekündigt. Er will dabei die europäischen Reformen berücksichtigen und die Rechte der betroffenen Personen stärken. Zudem seien die Kompetenzen der Datenschutzbehörde zu überprüfen und bereichsspezifisch die Einführung von «Best Practices»-Richtlinien zu erwägen. Generell wird es bei der Revision darum gehen, die Wirkung des DSG zu stärken und eine Verwesentlichung des Gesetzes zu erreichen, indem auf bürokratische Vorgaben verzichtet wird.

Revision des IDG

Die genannten Revisionen werden den Zeitplan und den Umfang einer Revision des IDG wesentlich bestimmen. Unzweifelhaft werden die Schengen-relevanten Bestimmungen umzusetzen sein. Des Weiteren geht es aber auch darum, die Erkenntnisse aus der Evaluation des IDG (Seite 14) entsprechend zu berücksichtigen. Nicht zuletzt wird auch zu überprüfen sein, wie die Bestimmungen zum Öffentlichkeitsprinzip noch besser in ein Gesamtbild integriert werden können. Neue Anforderungen, wie sie sich beispielsweise bei Open Government Data zeigen, werden zu berücksichtigen sein.

In einem ersten Schritt wird in einer Auslegeordnung der Handlungsbedarf aufzuzeigen sein. Daraufhin sind Lösungen zu diskutieren, wie auf diesen Handlungsbedarf mit konkreten Bestimmungen reagiert werden kann. Ziel muss es sein, das IDG den neuen Gegebenheiten und den Anforderungen der öffentlichen Organe an eine effiziente Datenbearbeitung anzupassen. Die Herausforderung liegt dabei im wirkungsvollen Schutz der persönlichen Freiheit und der Privatsphäre der Bürgerinnen und Bürger, dem Grundanliegen des IDG.

Impressum

Herausgeber: Datenschutzbeauftragter des Kantons Zürich, Postfach, CH-8090 Zürich
Lektorat: Text Control, Im Struppen 11, 8048 Zürich
Layout: René Habermacher, Visuelle Gestaltung, Flurstrasse 50, 8048 Zürich
Druck: Kantonale Drucksachen- und Materialzentrale (kdmz), Räffelstrasse 32, 8090 Zürich
Auflage: 900

ISSN 1422-5816

Kontakt

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

dsb

datenschutzbeauftragter
kanton zürich

www.datenschutz.ch

Datenschutz mit Qualität