dsb

datenschutzbeauftragter
kanton zürich

2016

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 2016 bis und mit 31. Dezember 2016 ab und wird im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, im April 2017

Der Datenschutzbeauftragte
des Kantons Zürich
Dr. Bruno Baeriswyl

«Der Fahrtwind in Richtung umfassende Digitalisierung hat zugenommen. Das Informations- und Datenschutzgesetz braucht deshalb angepasste Flügel. Ein Absturz beim Datenschutz wäre für alle Beteiligten fatal.»

Datenschutzbeauftragter des Kantons Zürich

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

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

- Bei öffentlichen Organen überprüft er mittels Kontrollen (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.

Inhaltsverzeichnis

«Die Kontrollen durch den Datenschutzbeauftragten sind ein geeignetes und wirkungsvolles Instrument, um die Anwendung der Datenschutzvorschriften durch die öffentlichen Organe sicherzustellen.»

Weichenstellung beim Datenschutz

Die Digitalisierung der Gesellschaft ist eine Chance für die öffentliche Verwaltung. Um unerwünschte Nebenwirkungen zu vermeiden, sind auch die Risiken zu eruieren und Rahmenbedingungen anzupassen, auch beim Datenschutz.

Mit dem Informations- und Datenschutzgesetz (IDG) hat sich der Kanton Zürich 2007 ein neues Gesetz gegeben, das den Datenschutz und das Öffentlichkeitsprinzip aufeinander abgestimmt regelt. Das IDG ersetzte das 1995 in Kraft getretene erste Datenschutzgesetz (DSG) des Kantons. Im vergangenen Jahr hat sich gezeigt, dass beim IDG aufgrund neuer Rechtsentwicklungen Anpassungsbedarf besteht. Der Datenschutzbeauftragte wirkte in der Arbeitsgruppe Datenschutz der Konferenz der Kantonsregierungen (KdK) mit, deren primäre Aufgabe es war, die Auswirkungen der Rechtsentwicklungen für die Kantone zu klären.

Europäische Rechtsentwicklungen

Zwei europäische Rechtsentwicklungen haben unmittelbaren Einfluss auf die kantonale Gesetzgebung:

- Der Europarat hat eine Anpassung der Konvention SEV 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten an die Hand genommen. Ein konsolidierter Text zur Modernisierung dieser Konvention wurde 2016 vorgelegt.
- Die EU hat die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen im Bereich Polizei und Justiz zusammen mit einer Datenschutzgrundverordnung 2016 verabschiedet.

Die Konvention SEV 108, welche die Schweiz 1997 ratifizierte, ist als Minimalstandard im Bereich des Datenschutzes zu betrachten. Sie ist von Bund und Kantonen in ihrer Gesetzgebung umzusetzen. Die Richtlinie im Bereich Polizei und Justiz ist sogenannt «Schengen-relevant», weshalb sie auch im schweizerischen Recht umzusetzen ist.

Der Bundesrat hat noch im Jahr 2016 eine Vernehmlassung zu einer Totalrevision des eidgenössischen Datenschutzgesetzes eröffnet. Damit nimmt er den Handlungsbedarf auf Bundesebene auf.

Vorarbeiten für den Kanton

Die Arbeitsgruppe Datenschutz der KdK hat diese Ausgangslage analysiert und auf der Basis der europäischen Gesetzestexte und des Vorschlags des Bundesrates den Handlungsbedarf für die Kantone im Einzelnen diskutiert. Daraus ist ein Leitfaden der Konferenz der Kantonsregierungen (KdK-Leitfaden) entstanden, der Anfang 2017 an die Kantonsregierungen verschickt wurde. Der KdK-Leitfaden enthält wichtige Hinweise für die Kantone, in welchen Bereichen eine Anpassung der Datenschutzgesetzgebung und eventuell weiterer Gesetze notwendig ist. Damit wird eine erste Weichenstellung für eine Revision des IDG vorgenommen.

Klare Rahmenbedingungen

Für den Kanton Zürich werden insbesondere die folgenden Punkte zu berücksichtigen sein:

Die öffentlichen Organe müssen einen Nachweis erbringen können, dass ihre Datenbearbeitungen dem IDG entsprechen. Eine Datenschutzfolgenabschätzung als Risikoanalyse hat einer Datenbearbeitung voranzugehen. Weiter bestehen Informationspflichten bei Datenschutzverletzungen.

An die Auftragsdatenbearbeitung werden konkretere Anforderungen gestellt.

Bürgerinnen und Bürger erhalten das Recht, aufsichtsrechtliche Anzeigen beim Datenschutzbeauftragten einzureichen. Der Datenschutzbeauftragte soll auch vorsorgliche Massnahmen aussprechen und Anordnungen erlassen können.

Der Geltungsbereich des IDG ist klarer zu regeln und Ausnahmen sind nur noch für privatwirtschaftlich handelnde öffentliche Organe (zum Beispiel die ZKB) zulässig. Im Übrigen gilt das IDG umfassend, wobei in hängigen Verfahren die individuellen Auskunftsrechte und die Aufsichtsrechte des Datenschutzbeauftragten beschränkt werden können.

Verschiedene Begrifflichkeiten, wie die biometrischen Daten, die genetischen Daten oder das Profiling, sind neu zu definieren.

Evaluation des IDG

Der Datenschutzbeauftragte hat in den vergangenen Jahren das IDG in einer umfassenden Weise evaluiert (Seiten 8 und 9). Die Ergebnisse der Evaluationssynthese werden bei einer Revision des IDG ebenfalls zu berücksichtigen sein.

Sicherheit der Daten

Im letzten Jahr hat sich gezeigt, dass die Daten der Verwaltung in zunehmendem Masse hohen Risiken ausgesetzt sind. Die Cyberrisiken haben generell zugenommen. Davon sind auch die öffentlichen Organe betroffen. Angriffe auf Systeme und Netzwerke haben zum Ziel, die Dienste zu blockieren oder Daten zu entwenden. Dabei kommt es immer häufiger zu erpresserischen Handlungen und oft gehören personenbezogene Daten zu den Zielen.

Im Rahmen der Revision des IDG ist deshalb auch zu prüfen, wie weit auf Gesetzesstufe konkretere Vorgaben in punkto Sicherheit für das Bearbeiten von Informationen und Daten zu erlassen sind. Auf jeden Fall genügen die in einer Verordnungsanpassung angedachten Massnahmen in keiner Art und Weise für einen angemessenen Schutz der Daten (Seite 33).

Digitalisierung als Herausforderung

Die Digitalisierung von Verwaltung und Gesellschaft bietet viele Chancen. Dafür müssen beim Datenschutz die Weichen richtig gestellt werden. Die Bürgerinnen und Bürger werden ihr Vertrauen in die staatlichen Datenbearbeitungen verlieren, wenn sie sich nicht mehr auf den Schutz ihrer Privatsphäre und die Sicherheit ihrer Daten verlassen können. Der Fahrtwind in Richtung umfassende Digitalisierung hat zugenommen. Das IDG braucht deshalb angepasste Flügel. Ein Absturz beim Datenschutz wäre für alle Beteiligten fatal.

Digitaler Tätigkeitsbericht

Die Digitalisierung macht auch nicht Halt vor gedruckten Publikationen. Erstmals liegt der Tätigkeitsbericht des Datenschutzbeauftragten nur noch in elektronischer Form vor. Damit kann er jederzeit konsultiert und bei Bedarf können der ganze Bericht oder einzelne Kapitel und Artikel ausgedruckt werden.

www.datenschutz.ch/TB2016

Evaluation IDG: Ergebnisse der Teilprojekte

Die Evaluation der Wirkungen des IDG, die 2012 mit der Erarbeitung eines Konzepts gestartet wurde, steht vor dem Abschluss. Die Ergebnisse der vier thematischen Teilprojekte werden nun in einer Synthese ausgewertet. Daraus wird ein allfälliger gesetzgeberischer Handlungsbedarf eruiert.

Das 2012 von der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) für den Datenschutzbeauftragten erstellte Konzept zur Evaluation des IDG (Tätigkeitsbericht 2012, Seite 12) sieht vor, die Wirkungen in vier Teilprojekten zu evaluieren: 1) Sensibilisierung der Bevölkerung, 2) Umsetzung des Gesetzmässigkeitsprinzips, 3) Öffentlichkeitsprinzip beziehungsweise erfüllte Informationspflicht der öffentlichen Organe und 4) Aufsicht Information/Datenschutz.

Die Sensibilisierung der Bevölkerung hinsichtlich Datenschutz und Öffentlichkeitsprinzip wurde 2013 evaluiert. Dazu war vom Statistischen Amt in Zusammenarbeit mit dem Link Institut eine Bevölkerungsbefragung durchgeführt worden (Tätigkeitsbericht 2013, Seiten 14 und 15). Das zweite Teilprojekt beinhaltete eine Analyse ausgewählter Gesetze zur Frage, ob die Erlasse hinreichend bestimmte Regelungen für sensible Datenbearbeitungen beinhalten (Tätigkeitsbericht 2014, Seiten 19 und 20). Dieses Teilprojekt wurde durch das Zentrum für Sozialrecht der ZHAW durchgeführt und 2015 abgeschlossen.

Umsetzung des Öffentlichkeitsprinzips

Für das dritte Teilprojekt, die Analyse der Umsetzung des Öffentlichkeitsprinzips, lud der Datenschutzbeauftragte die Koordinationsstelle IDG der Staatskanzlei als Kompetenzzentrum zu Fragen des Informationszugangs in der kantonalen Verwaltung zur Mitwirkung ein. Mit der Durchführung des Teilprojekts wurde das Statistische Amt beauftragt. Dieses bearbeitete Fragen in der zweiten Hälfte des Jahres 2016 einerseits im Rahmen einer Online-Befragung der öffentlichen Organe, andererseits mittels einer Internetrecherche und schloss das Teilprojekt mit einem Bericht Anfang 2017 ab.

Die Untersuchung der aktiven Informationstätigkeit der öffentlichen Organe zeigte, dass insbesondere die Gemeinden sehr aktiv informieren. Über Aufbau, Zuständigkeiten und Ansprechpersonen (§ 14 Abs. 2 IDG) informieren praktisch alle öffentlichen Organe. Das Verzeichnis der Informationsbestände (§ 14 Abs. 4 IDG) ist nur bei jedem fünften öffentlichen Organ publiziert und wurde in der Befragung häufig als wirkungslos und unnötig bezeichnet. Von besonderem Interesse waren die Antworten zum allgemeinen Informationszugangsrecht, das auch als Grundrecht in der Kantonsverfassung verankert ist (Art. 17 KV, § 20 Abs. 1 IDG). Es zeigte sich, dass die Anzahl schriftlicher Informationszugangsgesuche – soweit sie überhaupt als solche registriert werden – eher klein ist. Grös-

sere kantonale Stellen und Gemeinden sind häufiger mit solchen Gesuchen konfrontiert als kleinere. Bei rund einem Viertel der Gesuche findet aufgrund einer Interessenabwägung (§ 23 IDG) eine Einschränkung oder Verweigerung des Zugangs statt. Die Evaluation zeigte, dass das Öffentlichkeitsprinzip mehrheitlich problemlos umgesetzt werden kann, auch wenn teilweise die Interessenabwägung noch Schwierigkeiten bereitet und zusätzliche Vollzugshilfen gewünscht werden.

Aufsicht im Bereich Information und Datenschutz

Das vierte Teilprojekt der Evaluation befasste sich mit der Aufsicht in den Bereichen Information und Datenschutz und wurde von Interface Politikstudien im Herbst/Winter 2016/2017 durchgeführt. Nebst einer Auswertung von Grundlagen und Berichten des Datenschutzbeauftragten und von drei Vergleichsbehörden (Datenschutz- und Öffentlichkeitsbeauftragte der Kantone Basel-Stadt und Aargau sowie des Bundes) wurden mehrere Experteninterviews geführt.

Der Bericht zum Teilprojekt kommt zum Schluss, dass die Kontrollen durch den Datenschutzbeauftragten ein geeignetes und wirkungsvolles Instrument sind, um die Anwendung der Datenschutzvorschriften durch die öffentlichen Organe zu prüfen. Sie zeigten auf, dass bei den öffentlichen Organen im Kanton Zürich Vollzugsdefizite bestehen und selbst grundlegende Sicherheitsmassnahmen vielfach nicht umgesetzt werden. Den konkreten Defiziten im Vollzug können die Kontrollen jedoch nur zum Teil entgegenwirken, weil einerseits die Ressourcen für Kontrollen und Nachkontrollen beschränkt sind, andererseits die Hinweise und Massnahmen nur mangelhaft umgesetzt werden und dem Datenschutzbeauftragten die geeigneten Instrumente zur Durchsetzung fehlen.

Für die Aufsicht im Bereich Information und Öffentlichkeitsprinzip weist der Bericht auf erhebliche konzeptionelle Schwächen hin: Im Kanton Zürich ist keine Beratung von öffentlichen Organen ausserhalb der kantonalen Verwaltung für Medienschaffende oder Private zum Bereich Information und Öffentlichkeitsprinzip vorgesehen. Es besteht keine Stelle, welche über die Kompetenz verfügt, sich bei der Nichtgewährung von Informationszugangsgesuchen vermittelnd einzusetzen. Ausserdem fehlt innerhalb wie ausserhalb der kantonalen Verwaltung eine Stelle für die Umsetzung des Öffentlichkeitsprinzips.

Evaluationssynthese

Das Evaluationsprojekt wird in der ersten Hälfte 2017 mit einem Synthesebericht abgeschlossen. Die Ergebnisse der Evaluation dienen unter anderem als Grundlage für die anstehenden Revisionsarbeiten des IDG (Seiten 6 und 7). Das Konzept, die Berichte der Teilprojekte und der Synthesebericht sind auf der Website des Datenschutzbeauftragten verfügbar.
(www.datenschutz.ch > Rechtliche Grundlagen)

Entwicklungsschwerpunkte im KEF

Der Konsolidierte Entwicklungs- und Finanzplan (KEF) enthält nicht nur die Indikatoren und Messgrössen, die Angaben zur Erfüllung der gesetzlichen Aufgaben des Datenschutzbeauftragten machen, sondern auch jahresspezifische Schwerpunkte.

Die Indikatoren deuten auf eine weiterhin konstante Auslastung der Ressourcen. Sie bewegen sich in den vorgegebenen Zielgrössen, welche in Abhängigkeit von den beim Datenschutzbeauftragten zur Verfügung stehenden Mittel formuliert wurden. Neben den Leistungsindikatoren (siehe Zusammenfassung folgende Seite) werden auch zwei Wirkungsindikatoren aufgeführt.

Bei den Datenschutzreviews werden den öffentlichen Organen Hinweise gegeben, wie sie festgestellte Mängel beheben können. In der Regel wird eine Frist angesetzt, die in Abhängigkeit der Schwere des Mangels steht. Eine Kontrolle ist nachhaltig, wenn im Anschluss daran auch die entsprechenden Mängel behoben werden. Der Datenschutzbeauftragte kann hier beratend mitwirken. Auf seiner Website stellt er Hilfsmittel wie Checklisten zur Verfügung. Eine gute Wirkung der Kontrollen kann erzielt werden, wenn zwei Drittel der Hinweise umgesetzt werden. Zwar hat sich der Umsetzungsgrad gegenüber dem Vorjahr verbessert, doch liegt er mit rund einem Drittel der umgesetzten Hinweise immer noch weit unter dem gewünschten Mass. Der Datenschutzbeauftragte will deshalb die Nachkontrollen verstärken und hofft, dass die öffentlichen Organe sich vermehrt der Verantwortung für den Schutz und die Sicherheit der Daten der Bürgerinnen und Bürger bewusst werden. Diese sind mit der fortschreitenden Digitalisierung zunehmenden Risiken ausgesetzt.

Aus diesem Grund hat der Datenschutzbeauftragte im KEF für das Berichtsjahr die Förderung angemessener Massnahmen im Bereich der Informationssicherheit festgelegt. Es zeigte sich indessen, dass hierfür zu wenige Ressourcen zur Verfügung standen, um nachhaltig tätig werden zu können. So weit wie möglich wurde deshalb mittels Nachkontrollen und in Vernehmlassungsverfahren auf die Wichtigkeit einer angemessenen Informationssicherheit bei den öffentlichen Organen hingewiesen.

Mit zusätzlichen Entwicklungsschwerpunkten im KEF (Umgang mit grossen Datenmengen, regelmässige und nachhaltige Kontrollen) soll deshalb den festgestellten Mängeln bei der Informationssicherheit begegnet werden. Eine angemessene Sicherheit der Personendaten ist eine Grundvoraussetzung dafür, dass die Digitalisierung der Verwaltung als Chance genutzt werden kann. Allerdings sind hierfür zusätzliche Ressourcen unabdingbar.

KEF-Zahlen

Beratungen

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
2016	518

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
2016	14

Weiterbildung und Information

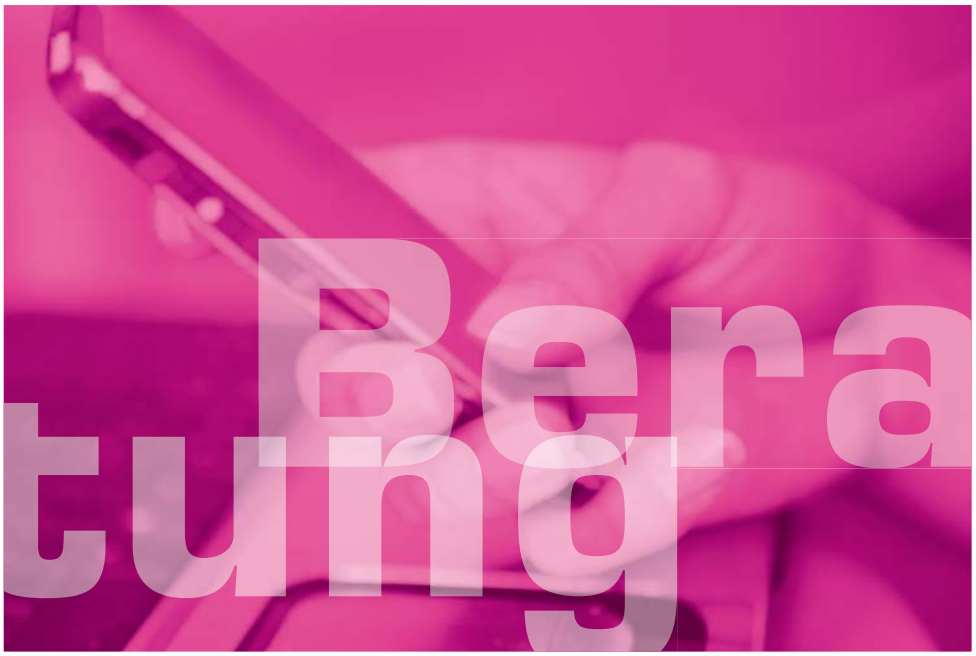
Der DSB bietet Aus- und Weiterbildungen im Bereich des Datenschutzes und der Informationssicherheit an. Dies erfolgt in der Form von internen oder externen Seminaren, Kursen, Workshops, Web-Trainingsprogrammen und Referaten. Der Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote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

KEF	20
2016	28

Kontrollen

Der DSB kontrolliert die Anwendung der rechtlichen, technischen und organisatorischen Vorschriften über den Datenschutz und die Informationssicherheit durch die öffentlichen Organe. Dazu führt er Datenschutzreviews durch, im Rahmen derer die Umsetzung der Anforderungen überprüft wird. Der Leistungsindikator im KEF gibt Auskunft über die realisierten Kontrollen.

KEF	40
2016	22



«Bei Bild- und Tonaufnahmen an Gemeindeversammlungen stehen der Grundsatz der Transparenz sowie die ungehinderte Ausübung der politischen Rechte im Vordergrund.»

Breites Themenspektrum

Gegenüber dem Vorjahr haben die Beratungen von Privatpersonen um rund 15 Prozent zugenommen. Sie liegen damit leicht über der Planzahl von 500 Beratungen. Die Beratungen von Bürgerinnen und Bürgern gehören zusammen mit den Beratungstätigkeiten für die öffentlichen Organe zu den Schwerpunkten im Tätigkeitsbereich des Datenschutzbeauftragten. Ihre Anzahl ist jedoch aufgrund der zur Verfügung stehenden Ressourcen limitiert. Eine im gleichen Umfang anwachsende Anzahl Beratungen – beispielsweise aufgrund der fortschreitenden Digitalisierung und der sich damit zunehmend stellenden Fragen in Bezug auf den Schutz und die Sicherheit der Daten – könnte nicht mehr bewältigt werden.

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
2016	518

Im Vordergrund stehen indessen die Beratungen der öffentlichen Organe. Das breite Spektrum der Themen erstreckt sich von der Frage nach den datenschutzrechtlichen Rahmenbedingungen bei Bild- und Tonaufnahmen an Gemeindeversammlungen über den Umgang mit Personendaten in der Forschung bis zur Auslagerung der Verlustscheinbewirtschaftung in der kantonalen Verwaltung.

Viele Fragen stellen sich neu, da die Informations- und Kommunikationstechnologie immer wieder neue Datenbearbeitungen ermöglicht. Insbesondere in Forschungsprojekten kommen diese bei Datenerhebungen und Auswertungen vorab zum Zuge. Mit der Information der betroffenen Personen über den Zweck des Forschungsvorhabens, der Möglichkeit, die Zustimmung zur Teilnahme zu geben oder zu verweigern, sowie den technischen Vorkehrungen zur rechtzeitigen Pseudonymisierung oder Anonymisierung der Personendaten lassen sich diese Forschungsvorhaben datenschutzkonform durchführen.

Zahlreiche Fragen stellen sich im direkten Zusammenhang mit dem Einsatz von bestimmten Softwareprodukten. Um den Prüfungsbetrug zu bekämpfen, wird Analysesoftware eingesetzt, oder um die Sicherheit der Netzwerkinfrastruktur zu gewährleisten, werden Tools angewendet, die verschlüsselte E-Mails entschlüsseln. Oft werden hier die datenschutzrechtlichen Vorgaben nicht standardmässig eingehalten. Deshalb müssen die Produkte entweder angepasst oder ausgetauscht werden.

01
Bild- und Tonaufnahmen an Gemeindeversammlungen

Eine Gemeinde wandte sich für die Vorprüfung einer kommunalen Verordnung zu Bild- und Tonaufnahmen bei Gemeindeversammlungen an den Datenschutzbeauftragten.

Der Entwurf hielt als Grundsatz fest, dass Bild- und Tonaufnahmen während der Gemeindeversammlung im Versammlungslokal nur von Personen gemacht werden dürfen, die vom Gemeinderat akkreditiert sind. Die Akkreditierung erfolgt in der Regel zum Zweck der Berichterstattung in den Medien und setzt voraus, dass die akkreditierte Person Gewähr für die Einhaltung der Verordnung bietet. Weiter enthielt die Verordnung Bestimmungen zum Verfahren der Akkreditierung, zur Zulässigkeit der Aufnahmen und zum Ausschluss von Aufnahmen im Einzelfall sowie zum Saalverweis.

Zudem hielt die Verordnung ein Aufnahmeverbot während Abstimmungen und Wahlen, ein Verbot von Live-Sendungen, eine Hinweispflicht auf die Aufnahmen sowie eine Strafbestimmung für Verstösse gegen die Verordnung fest. Eine dazu gehörende Akkreditierungsvereinbarung enthielt den ausdrücklichen Hinweis auf die Verpflichtung zur Einhaltung der gesetzlichen Bestimmungen durch die akkreditierten Personen, welche als private Datenbearbeitende dem eidgenössischen Datenschutzgesetz unterstehen.

Der Datenschutzbeauftragte prüfte die Verordnung und begrüsste den Erlass einer Rechtsgrundlage für Bild- und Tonaufnahmen an der Gemeindeversammlung. Bei solchen Aufnahmen stehen der Grundsatz der Transparenz sowie die Gewährung der politischen Rechte im Vordergrund. Mit einer transparenten Regelung entfällt das Erfordernis der vorgängigen Einwilligung durch die betroffenen Personen.

Ausserdem wahrt die Hinweispflicht auf die Aufnahmen das Transparenzprinzip. Die Verordnung sieht die Möglichkeit vor, dass aufgenommene Personen der Aufnahme widersprechen oder nachträglich deren Löschung verlangen können. Dadurch wird die Entscheidungsfreiheit der Betroffenen gewährleistet. Schliesslich wird auch der Schutz des Wahlgeheimnisses, der unverfälschten Stimmabgabe und der freien Meinungsbildung mit dem Aufnahmeverbot während Abstimmungen und Wahlen gewahrt.

§ 8 IDG
§ 12 IDG
Art. 34 BV

02
Auskünfte über konfessionsfremde Familienmitglieder

Ein Ehepaar erhielt zur Geburt seiner Tochter von der reformierten Kirche ein Schreiben, das nicht bloss an die Ehefrau, welche Mitglied dieser Kirche ist, sondern auch an die konfessionslose Tochter und den konfessionslosen Ehemann adressiert war. Die Einwohnerkontrolle bestätigte in der Folge gegenüber dem Ehemann die Bekanntgabe seiner Daten (Name, Vorname, Geburtsdatum, Adresse, Bürgerort und Beruf) sowie der Daten seiner Tochter an die Kirche. Der Ehemann wandte sich mit der Frage an den Datenschutzbeauftragten, ob eine solche Datenbekanntgabe zulässig sei.

Gemäss Kirchengesetz erhalten kantonale kirchliche Körperschaften und ihre Kirchgemeinden aus dem Einwohnerregister die zur Erfassung ihrer Mitglieder beziehungsweise zur Erfüllung ihrer kirchlichen Aufgaben benötigten Angaben. Wie die Kirchenverordnung konkretisiert, sind die Kirchgemeinden befugt, in Fällen, in denen nicht alle Personen einer Familie derselben kirchlichen Körperschaft angehören, über diese Personen Angaben aus dem Einwohnerregister zu beziehen. Das Kirchliche Datenschutz-Reglement enthält eine abschliessende Liste von Mitgliederdaten, die von der Einwohnerkontrolle an die Kirchgemeinde bekannt gegeben werden dürfen. Weitere Daten dürfen nur im Einzelfall bezogen werden und sind, wo immer möglich, bei der betroffenen Person direkt zu erheben.

Der Datenschutzbeauftragte stellte fest, dass nicht nur das Kirchliche Datenschutz-Reglement, sondern auch das Kirchengesetz und die Kirchenverordnung eine Auskunft der Einwohnerkontrolle gegenüber der Kirchgemeinde zu konfessionslosen Familienmitgliedern nur auf Anfrage und damit im Einzelfall zulassen. Auch der Regierungsrat spricht im Zusammenhang mit der Kirchenverordnung von «Auskünften» und weist damit auf die Voraussetzung einer Anfrage hin. Es kann folglich davon ausgegangen werden, dass der Gesetz- und Verordnungsgeber nicht über die Modalitäten der Datenbekanntgabe hinausgehen wollte, wie sie im Kirchlichen Datenschutz-Reglement festgehalten wurde. Systematische Datenlieferungen von konfessionslosen Familienmitgliedern durch die Einwohnerkontrolle an anerkannte Kirchgemeinden sind demnach nicht zulässig.

§ 16 IDG
§ 15 KiG
§ 3 Kirchenverordnung
§§ 3 und 4 Kirchliches Datenschutz-Reglement

03
Einsicht in Klassenauswertungen bei Schulevaluation

Ein Schulleiter wandte sich mit der Frage an den Datenschutzbeauftragten, ob er aufgrund seines gesetzlichen Auftrags zur personellen Führung Anspruch auf Einsicht in die im Rahmen der externen Schulevaluation erhobenen Klassenauswertungen habe.

Die Fachstelle für Schulbeurteilungen (FSB) evaluiert Volksschulen im gesetzlichen Auftrag, welcher sich auf die Schulen als Institution, nicht aber auf die einzelnen Klassen erstreckt. Dennoch wurden Klassen anhand von Eltern- und ab der 4. Klasse auch Schülerbefragungen evaluiert. Im Rahmen der Standardevaluation wurden Qualitätsmerkmale wie Unterrichts- und Klassenführung, individuelle Lernbegleitung, Beurteilung der Schülerschaft, Schulführung, Qualitätssicherung und entwicklung sowie Zusammenarbeit mit den Eltern beurteilt. Der Bildungsrat konnte diese Liste um aktuelle Merkmale erweitern.

War den Klassenlehrpersonen vor dem Bildungsratsbeschluss vom 9. März 2015 (BRB Nr. 11/2015), welcher auf Antrag der Bildungsdirektion gefällt wurde, die Teilnahme an der Evaluation freigestellt, können seitdem Schulen die Teilnahme anordnen. Anschliessend an die Evaluation erhalten die Klassenlehrpersonen die Möglichkeit, sich anhand eines Codes mit einem persönlichen Login zu registrieren und mittels per SMS zugestelltem PIN die Klassenauswertungen ihrer eigenen Klasse einzusehen. Der Bildungsrat entschied, den Schulleitungen keinen Zugang zu den Auswertungen der Klassenlehrpersonen zu gewähren. Ihnen wird lediglich in anonymisierter Form Auskunft über die Mittelwerte ihrer Klassen im kantonsweiten Vergleich erteilt. Jedoch ist im Bildungsratsbeschluss ausdrücklich festgehalten, dass die klassenbezogenen Auswertungen im Rahmen der Mitarbeiterführung von der Schulleitung eingesehen und so für die interne Qualitätssicherung und -entwicklung genutzt werden können.

Der Datenschutzbeauftragte bestätigte folglich den Anspruch des Schulleiters auf Einsicht in die Klassenauswertungen.

§ 8 IDG
§ 44 VSG

04

Schülerbefragung zu nationalen Bildungszielen

Im Rahmen des verfassungsmässigen Auftrags, die Bildungsziele zu harmonisieren, hat die Schweizerische Konferenz der kantonalen Erziehungsdirektoren (EDK) 2011 nationale Bildungsstandards verabschiedet. Diese beschreiben, welche Grundkompetenzen in einzelnen Fächern wie beispielsweise Mathematik oder Fremdsprachen bis zum Ende der obligatorischen Schule erreicht werden sollen. Die Daten für die Auswertung respektive Feststellung, ob die Grundkompetenzen in den Schweizer Schulen erreicht wurden, werden mit einem Fragebogen erhoben. Letzterer wird in ausgewählten Klassen an Schülerinnen und Schüler zum Ausfüllen verteilt.

Um differenzierte Aussagen über das Erreichen der Bildungsziele sowie über das Zustandekommen der Leistungen und Leistungsunterschiede machen zu können, finden sich in den Fragebogen auch Fragen, welche auf den ersten Blick nicht mit dem Erreichen dieser Grundkompetenzen in Zusammenhang gebracht werden können.

Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, hat unter Beteiligung des Datenschutzbeauftragten sowohl die Fragebogen als auch das Konzept und seine Umsetzung mit Blick auf datenschutzrelevante Aspekte geprüft.

Das Resultat hat ergeben, dass die Kantone, gestützt auf Bestimmungen des HarmoS-Konkordats, verpflichtet sind, diese Daten zu erheben. Wichtig in Bezug auf die befragten Schülerinnen und Schüler ist jedoch, dass das Ausfüllen auf freiwilliger Basis erfolgt und Transparenz über das Bearbeiten dieser Daten besteht, insbesondere über die Auswertungen, die Aufbewahrung und Löschung. Vorgeschlagen wurde, einzelne Fragen zu streichen, Daten teilweise zu anonymisieren und ein Datenschutzkonzept insbesondere betreffend Aufbewahrung und Löschung zu erarbeiten. All diese Punkte wurden umgesetzt. Weiter wurden die Eltern informiert sowie eine Website mit weiteren Informationen eingerichtet.

05

Schulärztliche Untersuchung durch Privatärztinnen und Privatärzte

Eine Kinderärztin wandte sich mit der Frage an den Datenschutzbeauftragten, ob das im Rahmen der Einführung der obligatorischen ärztlichen Gesundheitsvorsorge geschaffene «Gutscheinsystem» aus datenschutzrechtlicher Sicht zulässig sei. Dieses sieht vor, dass die Ärztin oder der Arzt nach der Untersuchung ein Rückmeldeformular an die Schulverwaltung und ein Befundformular an die Schulärztin respektive den Schularzt schickt.

Privatärztinnen und Privatärzte, die Kinder auf der Kindergartenstufe schulärztlich untersuchen, sind durch die Volksschulverordnung verpflichtet, den Schulgemeinden mitzuteilen, dass sie diese Untersuchungen durchgeführt haben. Auf dem Rückmeldeformular wie auf dem Befundformular sind Name, Vorname und Geburtsdatum des Kindes, Durchführungsdatum der Untersuchung und Angaben zur schulischen Einrichtung, welche das Kind besucht, auszufüllen. Beide Formulare erfragen zusätzlich Angaben zu verschiedenen Gesundheitsindikatoren. Für die Mitteilung dieser Untersuchungsresultate an die Schulverwaltung beziehungsweise den schulärztlichen Dienst wird in beiden Formularen das elterliche Einverständnis vorausgesetzt, ohne das die Fragen durch die Ärztin respektive den Arzt nicht beantwortet werden dürfen.

Der Datenschutzbeauftragte stellte fest, dass aufgrund der vorausgesetzten Einwilligung der Eltern das Gutscheinsystem datenschutzrechtlich zulässig ist. Die Ärztinnen und Ärzte können ihrer Pflicht, der Schulgemeinde die Durchführung der obligatorischen Untersuchung mitzuteilen, auch ohne die Beantwortung der Fragen zu den Gesundheitsindikatoren und damit unabhängig vom elterlichen Einverständnis nachkommen.

Schulen tragen die Verantwortung für die sichere Aufbewahrung der durch sie bearbeiteten Personendaten. Sie haben insbesondere sicherzustellen, dass der Zugriff auf die Daten auf jene Mitarbeitende beschränkt ist, welche diese Informationen zur Aufgabenerfüllung benötigen. Für die sichere Aufbewahrung der Befunde und Untersuchungsergebnisse sind die Ärztinnen und Ärzte zuständig.

§ 5 IDG
§ 8 IDG
§ 17 VSV
§ 17b VSV

06
Videoüberwachung im Spital

Der Datenschutzbeauftragte erhielt eine Meldung, wonach ein Spital auf der Kindernotfallstation an verschiedenen Standorten Videokameras installiert habe, unter anderem in den Behandlungszimmern. Videoüberwachungen in Behandlungsbereichen eines Spitals betreffen einen äusserst sensiblen Bereich. Der Datenschutzbeauftragte wandte sich deshalb zur Abklärung des Sachverhalts an das Spital. Er holte Auskünfte ein und besichtigte die Videoüberwachung auf Einladung des Spitals vor Ort.

Die Sachverhaltsabklärung ergab, dass das Spital die Videoüberwachung sowohl an allgemein zugänglichen Orten (z.B. Eingänge, Parkplatz, Flure) als auch in den Behandlungszimmern der Kindernotfallstation einsetzt beziehungsweise einsetzen möchte.

Die Videoüberwachung an allgemein zugänglichen Orten dient der Sicherheit und dem Schutz von Personen und Sachen. Der Datenschutzbeauftragte beriet das Spital in Bezug auf den Erlass eines Reglements, welches die Rahmenbedingungen der Videoüberwachung festhält und der Herstellung von Transparenz gegenüber den betroffenen Personen dient. Die Beurteilung der Verhältnismässigkeit der Videoüberwachung, namentlich die Prüfung, ob keine milderen Möglichkeiten zur Gewährleistung der Sicherheit und zum Schutz von Personen und Sachen bestehen, obliegt dagegen in erster Linie dem Spital.

Die Videoüberwachung in den Behandlungszimmern dient primär dem Schutz der Kinder. Gemäss Auskunft des Spitals kann es bei Kindern äusserst hilfreich sein, beim Entscheid über die Weiterbehandlung die Videoaufzeichnungen zu sichten, beispielsweise wenn sich der Gesundheitszustand des Kindes verschlechtert hat und zu diesem Zeitpunkt kein medizinisches Personal im Behandlungszimmer war. In der Ausgestaltung der Videoüberwachung als Echtzeitüberwachung dient sie der Überwachung des Gesundheitszustandes in speziellen Fällen, beispielsweise bei Kindern mit Epilepsie. Der Datenschutzbeauftragte gelangte zum Schluss, dass die Videoüberwachung in diesen Fällen ein Bestandteil der medizinischen Behandlung bildet und sich auf den Behandlungsauftrag abstützt. Zum Schutz der betroffenen Personen stellte er verschiedene Rahmenbedingungen auf, namentlich hinsichtlich der zu treffenden organisatorischen und technischen Massnahmen.

Das Spital möchte die Videoaufnahmen zudem zu Schulungs- und Fortbildungszwecken weiterverwenden. Die Weiterverwendung von Personendaten für einen anderen Zweck ist zulässig, sofern die betroffenen Personen damit einverstanden sind. Der Datenschutzbeauftragte prüfte die vom Spital definierten Prozesse zur Einholung der Einwilligungen und beriet dieses in Bezug auf die Anforderungen an eine rechtsgültige Einwilligung, die Verwaltung der Einwilligungserklärungen und der Videoaufzeichnungen sowie die Festlegung einer maximalen Aufbewahrungsdauer.

§ 8 IDG
§ 9 Abs. 1 IDG

07
Aufbewahrung von Patienten- und Forschungsakten

In einem Spital stellte sich die Frage, wie lange Patientendokumentationen und Forschungsakten aufbewahrt werden dürfen und ob sie dem zuständigen Archiv zur Übernahme angeboten werden müssen respektive abgeliefert werden dürfen. Zur Klärung dieser Fragen fand zunächst ein Austausch zwischen Vertreterinnen und Vertretern aus zwei Spitälern, der Gesundheitsdirektion, dem Staatsarchiv und der Kantonalen Ethikkommission Zürich statt. Der Datenschutzbeauftragte wurde anschliessend in die weitere Diskussion miteinbezogen.

Alle beteiligten Stellen waren sich einig, dass Patientendaten, die für die Behandlung erhoben und in der Patientendokumentation festgehalten wurden, nach Abschluss der letzten Behandlung während zehn Jahren aufbewahrt werden müssen. Die Aufbewahrungsfrist kann im Interesse der Patientin oder des Patienten oder für Forschungszwecke auf 30 Jahre oder, in Absprache mit dem zuständigen Archiv, auf 50 Jahre verlängert werden. Nach Ablauf der Aufbewahrungsfrist bieten Spitäler, welche öffentliche Aufgaben erfüllen, die Patientendokumentationen dem zuständigen Archiv zur Übernahme an. Patientendokumentationen, welche das Archiv nicht übernimmt, werden der Patientin oder dem Patienten herausgegeben oder vernichtet.

Weiter waren sich die beteiligten Stellen einig, dass ein Spital Patientendaten für Forschungszwecke weiterverwenden darf, sofern die Regelungen des Humanforschungsgesetzes eingehalten werden. In diesen Fällen entsteht eine Forschungsakte, welche aus einer Kopie der Patientendokumentation oder von Teilen daraus besteht (Datendoppel). Der Umgang mit Personendaten in Forschungsakten richtet sich nach dem Humanforschungsrecht. Weil dieses die Aufbewahrung von Personendaten, die für Forschungszwecke weiterverwendet werden dürfen, nicht regelt, darf das Spital die Daten so lange aufbewahren, als dies für Forschungszwecke geeignet und erforderlich ist beziehungsweise die Patientin oder der Patient ihre beziehungsweise seine Einwilligung nicht widerrufen hat. Offen blieb die Frage der Archivierung von Forschungsakten, da rechtliche Aspekte der Klärung bedürfen.

§ 18 ff. Patientinnen- und Patientengesetz
§ 8 Archivgesetz
Art. 33 f. Humanforschungsgesetz

08
Umgang mit Personendaten in der Forschung

Der Datenschutzbeauftragte befasste sich im Berichtsjahr mit verschiedenen Anfragen zu Datenbearbeitungen in Forschungsprojekten respektive für Forschungszwecke.

Ein Institut gelangte an den Datenschutzbeauftragten, weil es die von ihm gesammelten Personendaten einem Dritten zur Auswertung für ein Forschungsprojekt zur Verfügung stellen wollte. Bekannt gegeben werden sollten neben den für das Forschungsprojekt relevanten «Inhaltsdaten» das Geburtsdatum, das Geschlecht, die Nationalität und die Postleitzahl des Wohnorts der betroffenen Personen. Der Datenschutzbeauftragte erläuterte die Voraussetzungen für die Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck und wies darauf hin, dass es sich vorliegend nach wie vor um Personendaten handle, da eine Vielzahl der betroffenen Personen anhand des Geburtsdatums, des Geschlechts und der Postleitzahl bestimmbar seien.

In einem anderen Forschungsprojekt ging es darum, dass Jugendliche im Alter zwischen 12 und 19 Jahren während eines Monats den Umgang mit ihrem Smartphone in Tagebuchform dokumentieren und anschliessend dazu befragt werden. Zentral für die Mitwirkung von Jugendlichen im Forschungsprojekt ist deren Freiwilligkeit. Dies bedeutet, dass Jugendliche respektive ihre gesetzlichen Vertreterinnen oder Vertreter vorgängig über das Forschungsprojekt angemessen informiert werden müssen und ihre Einwilligung frei erteilen. Bei der Frage, von wem die Einwilligung einzuholen ist, ist massgebend, ob die betroffene Person urteilsfähig ist. Urteilsfähige Jugendliche erteilen ihre Einwilligung selbst. Der Datenschutzbeauftragte riet, den Eltern dennoch ein Schreiben zu senden, welches über die Teilnahme am Projekt und die damit verbundene Datenbearbeitung informiert. Bei urteilsunfähigen Jugendlichen ist die Einwilligung vom gesetzlichen Vertreter einzuholen. Zusätzlich sind auch die Jugendlichen in altersgerechter Form über das Projekt und die damit verbundene Datenbearbeitung aufzuklären.

Weiter wandte sich eine ausserkantonale Hochschule an den Datenschutzbeauftragten, da sie zur Durchführung einer Studie von verschiedenen öffentlichen Organen des Kantons Zürich Daten erheben wollte. Der Datenschutzbeauftragte äusserte sich dazu, unter welchen Voraussetzungen öffentliche Organe des Kantons Personendaten für ein Forschungsprojekt zur Verfügung stellen dürfen. Da es sich um die Bekanntgabe sensibler Daten handelte und diese neben dem Amtsgeheimnis auch spezialgesetzlichen Schweigepflichten unterliegen können, kam der Datenschutzbeauftragte zum Schluss, dass die Daten ausschliesslich anonymisiert bekannt gegeben werden dürfen. In den Gesuchen um Teilnahme am Forschungsprojekt war entsprechend darauf hinzuweisen. Die Hochschule kam diesen Anforderungen nach und dokumentierte den Datenschutzbeauftragten mit den entsprechenden Unterlagen.

Schliesslich wandte sich ein Spital an den Datenschutzbeauftragten mit dem Anliegen, ein von ihm geführtes Register, welches Forschungszwecken dient, mit Daten einer externen Rettungsorganisation auszubauen. Die Rettungsorganisation liefert Patientinnen und Patienten ins betreffende Spital ein. Es ging somit um die Frage, unter welchen Voraussetzungen Daten über eine Person, welche in beiden Institutionen behandelt worden war, für Forschungszwecke zusammengeführt werden dürfen. Beide Institutionen hatten die Daten in ihren Forschungsdatenbanken in pseudonymisierter Form gespeichert. Der Datenschutzbeauftragte prüfte die

Sach- und Rechtslage und kam zum Schluss, dass es sich bei den Daten der Rettungsorganisation aus Sicht des Spitals nicht um pseudonymisierte, sondern um identifizierende Daten handelt, da davon auszugehen ist, dass das Spital über den Schlüssel zur Re-Identifizierung der betroffenen Personen verfügt. Die Weitergabe der Daten von der Rettungsorganisation ans Spital unterliegt deshalb den Vorschriften über die Weiterverwendung von nichtgenetischen gesundheitsbezogenen Personendaten zu Forschungszwecken in identifizierender Form und bedarf der aufgeklärten Einwilligung der betroffenen Personen respektive der Bewilligung der Kantonalen Ethikkommission Zürich bei Daten von verstorbenen Personen.

§§ 18 und 23 IDG
§ 21 IDV
Art. 19c ZGB
Art. 33 f. HFG

09
Digitalisierung der Patientenakten

Ein Spital gelangte an den Datenschutzbeauftragen, um ein Projekt zur einheitlichen digitalen und rechtskonformen Archivierung von Patientenakten beurteilen zu lassen. Das Projekt sieht vor, elektronische Daten direkt aus dem Klinikinformationssystem zu archivieren wie auch Patientenunterlagen in Papierform zu digitalisieren.

Bei der klassischen Aktenführung (Papierdossiers) wie auch der elektronischen Aktenführung müssen bestimmte Anforderungen eingehalten werden. Zu beachten ist, dass
- die Vertraulichkeit gewahrt ist,
- die Daten bei Bedarf vorhanden sind,
- jede Datenbearbeitung (Erhebung, Veränderung, Löschung usw.) erkennbar und nachvollziehbar ist und einer Person zugerechnet werden kann,
- das Recht auf Zugang zu den eigenen Personendaten gewährt werden kann,
- die Daten richtig und vollständig sind und berichtigt werden können,
- nicht mehr benötigte Personendaten vernichtet werden.

Die vom Datenschutzbeauftragen beurteilten Dokumente bilden eine gute Grundlage für die Weiterentwicklung zu einem Detailkonzept. Die nötigen Prozesse für den Einsatz eines Ablagesystems und die darin abgelegten Dossiers sowie der Lebenszyklus eines digitalen Dossiers sind im Detailkonzept zu beschreiben. Ein besonderes Augenmerk gilt der Gewährleistung der Nachvollziehbarkeit und der Integrität. Es sind Protokolle zu führen, so dass nachgewiesen werden kann, ob eine Information in der Ablage verändert wurde. Für den Schutz und die Sicherung der Protokolle gelten die gleichen Anforderungen wie für die Dossiers selbst. Zudem müssen die ruhende Ablage und die Archivierung (Übergabe an das Staatsarchiv) eines Dossiers sowie die sachgerechte Vernichtung beziehungsweise Löschung unter Beachtung der dazugehörenden Fristen definiert werden.

§§ 5 IDG
7 IDG
§§ 13 Gesundheitsgesetz
§ 17 ff. Patientinnen- und Patientengesetz
ISV

10
Informationsaustausch zwischen Psychiatrie, Polizei und Staatsanwaltschaften

Die Gesundheitsdirektion hat eine Wegleitung für den Informationsaustausch zwischen Polizei, Staatsanwaltschaften und psychiatrischen Kliniken ausgearbeitet und sie dem Datenschutzbeauftragten zur Stellungnahme unterbreitet.

Die Wegleitung wurde in Zusammenarbeit mit der interdisziplinären Fachkommission für die Entwicklung von Handlungsstrategien zur Verbesserung des institutionen- und behördenübergreifenden Umgangs mit gewaltbereiten Personen erstellt und zeigt die rechtlichen Rahmenbedingungen für den Datenaustausch auf, insbesondere in Zusammenhang mit der Unterbringung und Behandlung gewaltbereiter Personen. Sie stellt dar, unter welchen Voraussetzungen Anfragen beziehungsweise Auskünfte erlaubt sind, wann Meldungen aus eigenem Antrieb zulässig sind und unter welchen Voraussetzungen eine direkte Zusammenarbeit zwischen den beteiligten Behörden möglich ist. Dabei ist insbesondere wesentlich, ob sich eine Person freiwillig oder aufgrund einer fürsorgerischen Unterbringung in einer psychiatrischen Klinik aufhält. Checklisten im Anhang sollen die Mitarbeitenden in psychiatrischen Kliniken sowohl beim Einholen von Informationen bei Polizei und Staatsanwaltschaften als auch beim Erteilen von Informationen gegenüber Polizei und Staatsanwaltschaften unterstützen.

Der Datenschutzbeauftragte prüfte den Entwurf der Wegleitung und nahm zu einzelnen Punkten Stellung. Er begrüsste die Wegleitung und beurteilte sie als ausgewogen und den Schutz der Privatsphäre betroffener Personen angemessen berücksichtigend. Er erachtet die Wegleitung als wertvolles Hilfsmittel für einen datenschutzkonformen Informationsaustausch zwischen den beteiligten Behörden.

Die Gesundheitsdirektion berücksichtigte die Hinweise des Datenschutzbeauftragten, insbesondere die Präzisierung, dass standardmässige Datenflüsse zwischen den beteiligten Behörden ausgeschlossen sind. Die Wegleitung ist auf der Website der Gesundheitsdirektion verfügbar.

§ 17 IDG
§ 23 IDG
§ 51 Personalgesetz
§ 15 Gesundheitsgesetz
Art. 451 ZGB
Art. 320 und 321 StGB

11
Einsicht in Laborunterlagen

Eine Privatperson wandte sich mit Fragen zur Einsicht in Unterlagen einer Laboruntersuchung an den Datenschutzbeauftragten. Sie hatte beim Institut, das die Untersuchung durchgeführt hatte, Auskunft über die einzelnen Laborwerte einer Blutuntersuchung ihres Kindes verlangt.

Der Datenschutzbeauftragte erläuterte der Privatperson den Anspruch auf Zugang zu den eigenen Personendaten. Zudem wies er sie darauf hin, dass bei urteilsunfähigen Personen das Auskunftsrecht durch den gesetzlichen Vertreter wahrzunehmen sei. Für das weitere Vorgehen verwies er auf die Ausführungen in seiner Broschüre «Meine Rechte» und machte auf die Mustervorlage für das Stellen eines Auskunftsgesuchs auf seiner Website www.datenschutz.ch aufmerksam.

In der Folge stellte die Privatperson ein Gesuch gestützt auf § 20 Abs. 1 IDG (Anspruch auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen) statt auf § 20 Abs. 2 IDG (Anspruch auf Zugang zu den eigenen Personendaten) und ohne Beilage der erforderlichen Ausweiskopien. Dies führte zu Rückfragen des Instituts, was von der Privatperson als Verweigerung der Herausgabe der gewünschten Unterlagen aufgefasst wurde. Der Datenschutzbeauftragte erklärte ihr den Unterschied zwischen den beiden Rechtsansprüchen, also dem Auskunftsrecht als Ausfluss aus dem Recht auf informationelle Selbstbestimmung und dem Recht auf Informationszugang als Ausfluss aus dem Öffentlichkeitsprinzip. Er führte aus, dass das Vorgehen des Instituts dazu diene, ihr Gesuch formal korrekt zu behandeln. Er empfahl der Privatperson, dem Institut mitzuteilen, dass sich das Gesuch richtigerweise auf § 20 Abs. 2 IDG stütze, und ihm die gewünschten Ausweiskopien zur Feststellung ihrer Identität und des gesetzlichen Vertretungsrechts zuzusenden.

§ 20 Abs. 1 und 2 IDG

12
Online-Portal einer Berufsschule

Eine Berufsschule wandte sich für die Prüfung der Nutzungs- und Datenschutzrichtlinie für ein Online-Portal an den Datenschutzbeauftragten. Das Online-Portal sei eine dynamische Kommunikationsplattform für Lernende, Lehrpersonen, Dozierende, Mitarbeitende und Kommissionsmitglieder der Berufsschule und biete nicht nur Informationsmöglichkeiten, sondern erlaube auch einen spielerischen, interaktiven Austausch zwischen den verschiedenen Nutzenden sowie eine aktive Teilnahme am Lernenden-Alltag und an der Weiterentwicklung der Schule. Der Entwurf der Richtlinie enthielt Bestimmungen über den Geltungsbereich, die Zustimmung zur Richtlinie, zu den Pflichten der Nutzenden sowie Sanktionen bei Nichtbeachtung, zum Datenschutz und zur Haftung sowie eine Einwilligungserklärung.

Wenn eine Schule eine Plattform betreibt, über die Personendaten bearbeitet werden, ist sie verpflichtet, diese Informationen durch angemessene organisatorische und technische Massnahmen zu schützen. Im Sinne der Transparenz sind die Nutzenden der Website darüber zu informieren, welche Personendaten bei der Nutzung der Plattform erhoben werden, durch wen und zu welchem Zweck sie bearbeitet werden, ob sie an Dritte bekannt gegeben und wie lange sie aufbewahrt werden.

Der Datenschutzbeauftragte prüfte die Richtlinie und wies die Schule darauf hin, dass die Nutzenden die Inhalte jederzeit löschen können müssen. Es muss gewährleistet sein, dass die gelöschten Inhalte vollständig aus dem Portal entfernt werden. Weiter machte er darauf aufmerksam, dass in der Richtlinie ein Hinweis fehlt, was mit den Benutzerprofilen von Schülerinnen und Schülern sowie von anderen Nutzenden passiert, welche aus der Schule austreten. Hierfür hat er als Möglichkeit vorgeschlagen, dass die Profile bei Austritten automatisch gelöscht und die Nutzenden darauf aufmerksam gemacht werden, dass sie selber verantwortlich sind, ihre Inhalte vom Portal auf persönliche Speichermedien zu übertragen.

§ 7 IDG
§ 12 IDG

13
Analysesoftware gegen Prüfungsbetrug

Eine Fachhochschule wandte sich mit der Frage an den Datenschutzbeauftragten, ob und unter welchen Bedingungen Analysetools zur Aufdeckung von Betrugsfällen bei Prüfungen eingesetzt werden dürfen, an denen die Studierenden ihre privaten Computer verwenden.

Die Verordnung zum Fachhochschulgesetz und die Fachhochschulordnung erlauben der Fachhochschule, Massnahmen zur Aufdeckung von Prüfungsbetrug zu treffen. Beim Einsatz eines Analysetools zur Verhinderung von Prüfungsbetrug muss darauf geachtet werden, dass es entsprechend dem Grundsatz der Verhältnismässigkeit geeignet und erforderlich ist (§ 8 Abs. 1 IDG). Es darf nur eingesetzt werden, wenn keine Massnahmen bestehen, die weniger in die Privatsphäre einschneiden und für die Erreichung des Zwecks ebenfalls zielführend wären. Zeitlich sind das Loggen auf die Prüfungsdauer und dessen Umfang auf die auf Prüfungsbetrug hindeutenden Aktivitäten zu beschränken. Das Überprüfen von Zugriffen auf Websites oder auf Kommunikationsplattformen erscheint verhältnismässig. Das Aufzeichnen von auf dem persönlichen Computer abgelegten Daten ist aber einzuschränken. Spätestens nach der Auswertung müssen die gesammelten Personendaten vernichtet werden. Eine Aufbewahrung von Log-Dateien rechtfertigt sich nur bei konkreten Hinweisen auf einen Betrugsfall.

Die Studierenden müssen ausserdem aus Transparenzgründen angemessen über Umfang und Zweck des Einsatzes eines Analysetools bei der Verwendung des eigenen Computers an den Prüfungen aufgeklärt werden. Aufgrund der fehlenden Rechtsgrundlage zur Verwendung privater Computer müssen die Studierenden wählen können, ob sie private oder von der Schule zur Verfügung gestellte Geräte verwenden wollen. Die alternativ zur Verfügung gestellten schulischen Geräte sind so zu konfigurieren, dass keine Überwachung nötig ist (privacy by default).

Die Fachhochschule muss ihre Informationen durch angemessene organisatorische und technische Massnahmen schützen. Falls sie die Software eines Anbieters in Anspruch nehmen möchte, welche eine Cloud-Lösung beinhaltet oder bei welcher der Anbieter Zugriff auf die Logdateien hat, sind die Voraussetzungen für das Bearbeiten im Auftrag zu prüfen.

§ 6 IDG
§ 7 IDG
§ 8 IDG
§ 12 IDG
§ 25 IDV

14

Zentralisierung und Auslagerung der Verlustscheinbewirtschaftung

Die Finanzverwaltung wurde vom Regierungsrat beauftragt, die Bewirtschaftung der Verlustscheine neu zu organisieren (RRB 236/2016). Einerseits sollen diese zentral für den Kanton bewirtschaftet und andererseits soll eine Auslagerung dieser Tätigkeit an Dritte geprüft werden. Ausgenommen werden Behörden, welche die Verlustscheine selbst bewirtschaften möchten.

Der Datenschutzbeauftragte wurde um Überprüfung der Rechtslage angefragt. Was die Auslagerung selbst betrifft, ist diese durch die Bestimmungen im IDG gedeckt, und zwar sowohl die Auslagerung der Datenbearbeitungen anderer Behörden, aber auch von nicht dem Regierungsrat unterstellten Stellen an die Finanzdirektion als auch die Auslagerung der Datenbearbeitung der Finanzdirektion an ein privates Unternehmen. Dies gilt auch, wenn sich diesem Vorhaben selbstständige Anstalten anschliessen möchten. Nicht geprüft wurde in diesem Kontext die Frage, ob die Finanzdirektion diese Bewirtschaftung für alle kantonalen Organe und selbstständigen Anstalten durchführen darf. Dies ist eine Frage der Kompetenzen und liegt somit ausserhalb des datenschutzrechtlichen Kontextes.

Wichtig bei der Auslagerung einer Datenbearbeitung ist, dass die Behörde, welche den Auftrag für die Datenbearbeitung an Dritte erteilt, für die Informationen verantwortlich bleibt. Weiter ist zu berücksichtigen, dass eine Auslagerung von Daten, welche dem Berufsgeheimnis von Art. 321 StGB unterstehen, grundsätzlich nur mit Einwilligung respektive mit Information der Betroffenen erfolgen kann, denn eine Verschlüsselung der Daten, wie sie in anderen Bereichen vorgenommen werden kann, kommt in diesem Fall nicht in Betracht.

Ob die Verlustscheinbewirtschaftung innerhalb des Kantons zentral stattfindet oder an ein Privatunternehmen ausgelagert wird, macht für die datenschutzrechtliche Beurteilung keinen Unterschied. Beim Insourcing kommen im Gegensatz zum Outsourcing andere, in der Regel weniger weit gehende organisatorische und technische Sicherheitsmassnahmen zum Tragen.

§ 6 IDG
§ 25 IDV

15
Secure Web Access für die kantonale Verwaltung

Der Datenschutzbeauftragte wurde von einer Direktion angefragt, den mit einem externen Auftragnehmenden abgeschlossenen Vertrag über den Webzugang des Kantons mittels einer Cloud-Lösung eines Drittanbieters (Sub-Auftragnehmender) auf die datenschutzrechtlichen Aspekte zu prüfen.

Ruft eine Mitarbeiterin oder ein Mitarbeiter der kantonalen Verwaltung eine Website auf, geschieht dies über einen zentralen Internet Surf Proxy. Der Internet Surf Proxy prüft, ob die aufgerufene Website den Richtlinien entspricht und keine sicherheitskritischen Elemente wie zum Beispiel Viren enthält. Entspricht eine Website den Richtlinien, kann die Benutzerin oder der Benutzer die Website ansehen, sonst wird sie blockiert. Neben den eigentlichen Inhaltsdaten der Website fallen zahlreiche Randdaten an wie das Datum des Zugriffs oder die Websiteadresse. Der externe Auftragnehmende (Provider) ist verpflichtet, diese Randdaten während sechs Monaten aufzubewahren.

Die Rand- und Inhaltsdaten sind als besondere Personendaten einzustufen, da sie mit anderen Informationen verknüpft werden können und so die Erstellung eines Persönlichkeitsprofil ermöglichen. Durch die Auslagerung einzelner Teile der Dienstleistung des Auftragnehmenden an einen Sub-Auftragnehmenden in den USA, welcher die Cloud-Lösung anbietet, findet eine Datenbearbeitung im Ausland statt, die durch die Auftraggeberin ausdrücklich genehmigt werden muss.

Der Kanton nutzt die Möglichkeit, gewisse verschlüsselte TLS/SSL-Verbindungen (https) auf dem Internet Surf Proxy zu terminieren und auch den Inhalt auf sicherheitskritische Elemente zu überprüfen. Die Entschlüsselung von TLS/SSL-Verbindungen ist für die Mitarbeitenden transparent zu machen und es sind die nötigen Prozesse zu definieren sowie die entsprechenden organisatorischen und technischen Massnahmen zu treffen.

Das aktuelle Konzept für den Webzugang der Verwaltung erfüllt die rechtlichen, organisatorischen und technischen Anforderungen, insbesondere die gemäss Ausschreibung geforderte und im technischen Leistungsumfang beschriebene Datenhaltung in der Schweiz, nur teilweise. Die Lösung ist deshalb nachzubessern.

§ 6 IDG
§ 7 IDG
§ 12 IDG
§ 10 ISV
§ 34 Abs. 1 Personalgesetz
Art. 15 Abs. 3 BÜPF
§ 75 Vollzugsverordnung zum Personalgesetz
§§ 2 ff. Verordnung über die Nutzung von Internet und E-Mail
§§ 10 ff. Verordnung über die Nutzung von Internet und E-Mail

«Der einfachere, digitalisierte Leistungsbezug von Bevölkerung, Wirtschaft und anderen setzt Vertrauen in einen angemessenen Schutz der Daten voraus.»

Informationssicherheit bleibt ein Thema

Auch im Berichtsjahr hat der Datenschutzbeauftragte verschiedene Mitberichte und Stellungnahmen in Vernehmlassungsverfahren abgegeben. Die Anzahl der Vernehmlassungen kann der Datenschutzbeauftragte nicht beeinflussen, sie bewegt sich aber immer um den festgelegten Zielwert von 18 Stellungnahmen und Mitberichten. 2015 waren es 23, im vergangenen Jahr 14.

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
2016	14

Die Gesetzesvorhaben sind aus datenschutzrechtlicher Sicht unterschiedlich relevant. Insbesondere das Bearbeiten von sensitiven Personendaten braucht aber klare Rechtsgrundlagen, welche die Datenbearbeitungen für die betroffenen Personen nachvollziehbar machen.

Mit der fortschreitenden Digitalisierung tritt vermehrt die Sicherheit der Daten in den Vordergrund. Die kantonale Verwaltung tut sich schwer, hier die notwendigen Rahmenbedingungen zu schaffen. Eine neue Informationssicherheitsverordnung und ein Reglement zur Informationsverwaltung, die im Jahr 2015 in der Vernehmlassung waren, wurden 2016 in einer Verordnung über die Informationsverwaltung und -sicherheit zusammengefasst. Der Datenschutzbeauftragte wies in seiner Vernehmlassungsantwort darauf hin, dass die geplante Verordnung einen Rückschritt in Bezug auf die geltende Informatiksicherheitsverordnung bedeutet. Sie verpasst es, Vorgaben zu machen, so dass ein einheitliches Sicherheitsniveau in der Verwaltung entsteht. Vielmehr überlässt sie die Beurteilung des Sicherheitsniveaus den einzelnen öffentlichen Organen, die – wie Kontrollen zeigen – sich der Risiken für ihre Daten oft nicht bewusst sind.

Angesichts der zunehmenden Digitalisierung und der zunehmenden Risiken bezüglich den Schutz und die Sicherheit der Daten stellte der Datenschutzbeauftragte in der Vernehmlassung fest, dass die geplante Verordnung ungenügend ist. Er riet von einer Verabschiedung ab.

Vernehmlassungen

Der Datenschutzbeauftragte hat 2016 unter anderem zu folgenden Gesetzgebungsprojekten Stellung genommen:

Kanton

– Teilrevision des Verordnungsrechts zum kantonalen Geoinformationsgesetz
– Leitfaden zur Zusammenarbeit zwischen den Schulen und den Kindes- und Erwachsenenschutzbehörden (KESB)
– Umsetzungsvorschlag zur Motion KR-Nr. 251/2014 «Ein Betreibungsregister für den Kanton Zürich»
– Datenschutzverordnung der Universität (Neuerlass)

Bund

– Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier
– Weiterentwicklung des Datenschutzrechts der Europäischen Union

Ungenügende Verordnung über die Informationsverwaltung und -sicherheit

Der Datenschutzbeauftragte hat bei den Revisionsarbeiten der Informatiksicherheitsverordnung (ISV) wie bei den Arbeiten zum Erlass von Regelungen zur Informationsverwaltung mitgewirkt, Stellung zu Entwürfen genommen und auch auf Koordinationsbedarf hingewiesen (Tätigkeitsbericht 2015, Seiten 28, 32 und 33). Der daraufhin erarbeitete Entwurf einer Verordnung über die Informationsverwaltung und -sicherheit (VO IVS) wurde Ende 2016 in die Vernehmlassung gegeben. Der Datenschutzbeauftragte kam zum Schluss, dass der Entwurf in eine falsche Richtung weist.

Der Bericht über die unabhängige Überprüfung der Informatik des Kantons Zürich vom 31. Oktober 2016, den der Regierungsrat in Auftrag gegeben hatte, hält fest, dass grosse Bedenken bezüglich der Informationssicherheit bestehen. Er stellt infrage, ob bei einer derart vielfältigen und komplexen Informatik eine ausreichende Informationssicherheit ohne weitreichende Massnahmen gewährleistet werden kann. Der Regierungsrat hat die Schlussfolgerungen des Berichts in den wesentlichen Teilen als zutreffend bezeichnet und die Informationssicherheit als spezifisch anzugehende Fragestellung definiert. Auch der Datenschutzbeauftragte stellt bei seinen Kontrollen fest, dass ein grosser Nachholbedarf, selbst in Bezug auf die Grundschutzmassnahmen der Informationssicherheit, besteht.

Vor diesem Hintergrund ist die vorgeschlagene VO IVS ein nicht nachvollziehbarer Rückschritt. Die bisherige ISV aus dem Jahr 1997 ist zwar revisionsbedürftig, bietet aber den öffentlichen Organen einen weit besseren Orientierungsrahmen für die Informationssicherheit.

Zudem hält Art. 3 des neuen Informationssicherheitsgesetzes (ISG) des Bundes fest, dass das ISG auch für die Kantone gilt, wenn sie mit dem Bund zusammenarbeiten oder auf Informatikmittel des Bundes zugreifen. Es gilt nur dann nicht, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten. Dies ist mit der VO IVS nicht der Fall. So würde der Kanton Zürich bei Massnahmen in der Informationssicherheit in vielen Bereichen die Vorgaben des Bundes umsetzen müssen.

Auch in Bezug auf die vom Regierungsrat am 7. Dezember 2016 verabschiedete Strategie «Digitale Verwaltung» wird mit der VO IVS ein fragwürdiges Zeichen gesetzt. Insbesondere der einfachere, digitalisierte Leistungsbezug von Bevölkerung, Wirtschaft und anderen setzt Vertrauen in einen angemessenen Schutz der Daten voraus. Mit der VO IVS wird dieses Vertrauen in eine sichere Datenbearbeitung nicht gestärkt.

Der Datenschutzbeauftragte riet dem Regierungsrat, die Verordnung nicht zu verabschieden, die Revision des IDG abzuwarten (Seiten 6 und 7) und die einschlägigen Verordnungen im Zusammenhang mit dieser Revision anzupassen.

Zentrales Betreibungsregister für den Kanton

Mit der Motion KR-Nr. 251/2014 verlangte der Kantonsrat die Einrichtung eines zentral geführten Betreibungsregisters im Kanton. Der Datenschutzbeauftragte nahm zum Umsetzungsvorschlag im Einführungsgesetz zum Bundesgesetz über Schuldbetreibung und Konkurs (EG SchKG) Stellung. Er begrüsste den Erlass der Regelung in einem Gesetz im formellen Sinn. Wird ein elektronischer Zugriff auf ein Register (sogenannter Online-Zugriff) gewährt, bedarf dies einer formell-gesetzlichen Rechtsgrundlage.

Der Entwurf sah die Verwendung der AHV-Versichertennummer durch die Betreibungsämter als Identifikator vor. Die ursprünglich nur für den Bereich der Sozialversicherungen vorgesehene Nummer sollte auch im Bereich der Schuldbetreibung verwendet werden. Der Datenschutzbeauftragte sprach sich dagegen aus, die AHV-Versichertennummer durch einzelne gesetzliche Regelungen faktisch zu einem allgemein gebräuchlichen administrativen Personenidentifikator auszuweiten, weil dies die Risiken einer Persönlichkeitsverletzung für die betroffenen Personen erhöht.

Der Entwurf sah zudem vor, dass die Betreibungsämter die Daten von der kantonalen Einwohnerdatenplattform (KEP) beziehen. Das Gesetz über das Meldewesen und die Einwohnerregister des Kantons Zürich hält fest, dass die Betreibungsämter nur in ihrem örtlichen Zuständigkeitsbereich Daten elektronisch aus der KEP abrufen dürfen, soweit es für die Erfüllung ihrer gesetzlichen Aufgaben notwendig ist. Die Ausweitung dieser Befugnis mittels eines zentralen Registers erschien nicht erforderlich, weshalb der Datenschutzbeauftragte darauf hinwies, dass dieses Vorgehen unter dem Aspekt des Verhältnismässigkeitsgrundsatzes nochmals zu überprüfen sei.

Schliesslich hielt der Datenschutzbeauftragte in Bezug auf die Verantwortlichkeit für die Datenbearbeitung fest, dass die Verantwortlichkeiten zu regeln sind, wenn mehrere öffentliche Organe einen gemeinsamen Informationsbestand bearbeiten (insbesondere bei einem zentralen Register). Dies war im Entwurf nicht vorgesehen.

§ 17 Abs. 1 lit. a IDG
§ 23 Abs. 1 lit. a MERG
§ 5 Abs. 1 Satz 2 IDG i.V.m. § 1 IDV

Elektronisches Patientendossier

Am 19. Juni 2015 verabschiedete das Parlament das Bundesgesetz über das elektronische Patientendossier. Zur Ausführung des Bundesgesetzes erarbeitete der Bund drei Verordnungen, deren Entwürfe er im Berichtsjahr in die Anhörung gab. Der Datenschutzbeauftragte nahm im Rahmen des Mitberichtsverfahrens zuhanden der Gesundheitsdirektion zur Vorlage Stellung.
In datenschutzrechtlicher Hinsicht ist in erster Linie die Verordnung über das elektronische Patientendossier (EPDV) relevant.

Nach Ansicht des Datenschutzbeauftragten war die EPDV sorgfältig ausgearbeitet. Je nach Themenbereich berücksichtigte sie den Datenschutz unterschiedlich zufriedenstellend. Drei Themenbereiche, welche nicht oder nicht ausreichend geregelt wurden, waren die Zugriffsberechtigungen von Hilfspersonen des Gesundheitsfachpersonals, die datenschutzrechtliche Aufsicht über die (Stamm-) Gemeinschaften sowie die Vorgabe zur Verschlüsselung der Datenhaltung und -übertragung. Letztere stellt eine zentrale Vorgabe dar und sollte nach Ansicht des Datenschutzbeauftragten in der EPDV selbst und nicht nur im Anhang einer Departementsverordnung verankert werden. Weiter sprach sich der Datenschutzbeauftragte für das Festhalten an der Struktur des elektronischen Patientendossiers (ePD) mit den vier Vertraulichkeitsstufen und der Steuerung der Zugriffsrechte durch die Patientin respektive den Patienten aus. Den Patientinnen und Patienten ist beim Entscheid, wer welche Gesundheitsdaten über sie abrufen darf, grösstmögliche Freiheit einzuräumen, auch wenn dadurch die Komplexität erhöht wird. In diesem Zusammenhang regte der Datenschutzbeauftragte an zu überprüfen, ob die Grundeinstellungen im ePD aus einem Privacy-by-default-Ansatz restriktiver auszugestalten sind. Darüber hinaus äusserte er sich zu weiteren Aspekten, beispielsweise zur Anbindung von Primärsystemen an das ePD, zur Löschung von Daten aus dem ePD sowie zur Information der Patientin oder des Patienten über mögliche informationssicherheitsrechtliche Risiken bei der Nutzung des ePD.

Zusammenarbeit zwischen Schule und KESB

Der Datenschutzbeauftragte nahm zum «Leitfaden zur Zusammenarbeit zwischen den Schulen und den Kindes- und Erwachsenenschutzbehörden (KESB) bei Gefährdungen des Kindeswohls» Stellung. Der Leitfaden basiert auf den Grundsätzen der Zusammenarbeit zwischen den Schulen und den KESB bei Gefährdung des Kindeswohls, die durch die Bildungsdirektion, die Justizdirektion, die KESB-Präsidien-Vereinigung Kanton Zürich (KPV), den Verband Zürcher Schulpräsidien (VZS), den Verband Schulleiterinnen und Schulleiter Zürich (VSLZH) und die Vereinigung des Personals Zürcherischer Schulverwaltungen (VPZS) erstellt wurde. Inhalt des Leitfadens sind die Aufgaben von KESB, Schulen und Mandatspersonen, Ausführungen zur Gefährdung des Kindeswohls und die Gefährdungsmeldung an die KESB sowie die Zusammenarbeit zwischen Schule und KESB.

Der Datenschutzbeauftragte prüfte den Leitfaden und stellte fest, dass insbesondere der Verhältnismässigkeitsgrundsatz beachtet wird, indem nur Informationen ausgetauscht werden dürfen, welche für das empfangende Organ zur Erfüllung seiner Aufgaben geeignet und erforderlich sind. Zudem wird beim Austausch von Personendaten der Transparenz Rechnung getragen, indem die Betroffenen – wo dies den Zweck beispielsweise einer Meldung nicht vereiteln würde – vorgängig darüber benachrichtigt werden.

Weiter begrüsste der Datenschutzbeauftragte, dass ausdrücklich auf die vor der Einsichtsgewährung durchzuführende Interessenabwägung hingewiesen wird. Zudem umschreibt der Leitfaden Grundsätze für den sicheren Datentransfer. Der Datenschutzbeauftragte kam zum Schluss, dass der Leitfaden den Beteiligten eine ausgewogene Handlungsanleitung zur Verfügung stellt.

§ 8 IDG
§ 12 IDG
§ 23 IDG
§ 7 IDG

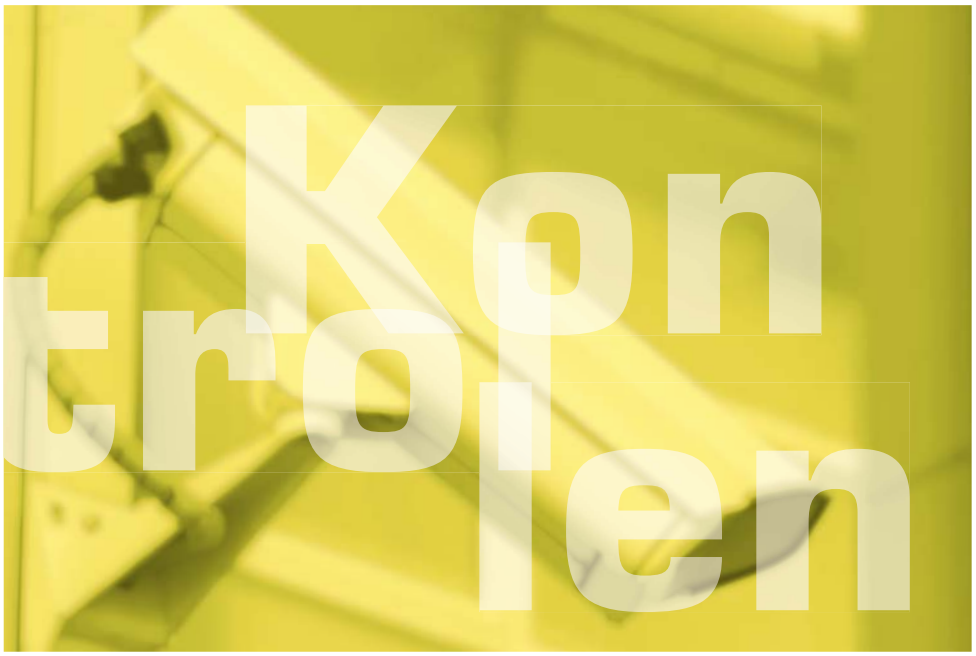
Weiterentwicklung des Datenschutzrechts

Im Berichtsjahr hat der Bund die Kantone betreffend die Datenschutzreformen in der EU und im Europarat konsultiert. Der Datenschutzbeauftragte hat dazu einen Mitbericht verfasst.

Die Weiterentwicklungen des europäischen Datenschutzrechts betreffen den Bund und die Kantone. Sie werden den Zeitplan und den Umfang der Revision des IDG wesentlich bestimmen.

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 der Strafvollstreckung sowie zum freien Datenverkehr», die an die Stelle des Rahmenbeschlusses 2008/977 treten wird, ist Schengen-relevant. Falls nicht das Risiko eingegangen werden soll, dass die Schengen-Assoziierung aufgelöst wird, muss die Schweiz die Richtlinie übernehmen. Das betrifft nicht nur den Bund, sondern auch die Kantone.

Die Informationsnotiz «Datenschutz: Übernahme von Rechtsakten. Ergänzende Ausführungen zur Konsultation des Bundes» der Konferenz der Kantonsregierungen (KdK) vom 17. Februar 2016 listet die wichtigsten Punkte auf, die tendenziell in der Datenschutzgesetzgebung der Kantone noch nicht so geregelt sind, wie es die neue Richtlinie vorsieht. In der Zwischenzeit wurden sie vom Leitfaden der KdK präzisiert. Die aufgeführten Punkte sind grösstenteils auch für das IDG relevant. Bisher wurde auf kantonaler Ebene darauf verzichtet, bloss bereichsspezifische Anpassungen vorzunehmen. Diese Vorgehensweise der Kantone hat sich bewährt, da in der Praxis ein Schengen-relevantes Datenschutzrecht neben einem allgemeinen Datenschutzrecht kaum vollziehbar wäre.



«Im Rahmen des Bedrohungsmanagements sind nur Datenbearbeitungen möglich, die durch bestehende Rechtsgrundlagen abgedeckt sind.»

Mit Kontrollen zu angemessener Sicherheit

Die Kontrolltätigkeit wird immer wichtiger. Regelmässig zeigt sich, dass die Massnahmen zur Sicherheit der Daten nur unvollständig umgesetzt sind. Dabei fehlt es oft an wesentlichen Grundschutzmassnahmen.

Aufgrund fehlender Ressourcen konnten im Berichtsjahr nicht alle Kontrollen durchgeführt oder zu Ende geführt werden, so dass die geplante Anzahl nicht erreicht wurde. Dabei hat sich auch gezeigt, dass der Aufwand für die einzelnen Kontrollen sehr unterschiedlich ist. Das Konzept der Datenschutz-Reviews wurde deshalb angepasst.

Der DSB kontrolliert die Anwendung der rechtlichen, technischen und organisatorischen Vorschriften über den Datenschutz und die Informationssicherheit durch die öffentlichen Organe. Dazu führt er Datenschutzreviews durch, im Rahmen derer die Umsetzung der Anforderungen überprüft wird. Der Leistungsindikator im KEF gibt Auskunft über die realisierten Kontrollen.

KEF	40
2016	22

Standardmässige Reviews beschränken sich auf die organisatorischen und technischen Grundschutzmassnahmen und ausgewählte rechtliche Überprüfungen. Liegt das Ergebnis unter einem akzeptablen Durchschnittswert, wird eine Nachprüfung in einem angemessenen Zeitabstand geplant. In jedem Fall werden für die Behebung der festgestellten Mängel Fristen festgelegt und das öffentliche Organ wird aufgefordert, über den Vollzug der Massnahmen dem Datenschutzbeauftragten Bericht zu erstatten. Im Berichtsjahr konnten erste Nachprüfungen durchgeführt werden.

Vertiefte Prüfungen finden in Bereichen statt, in denen sensitive Personendaten bearbeitet werden und eine grosse Anzahl Personen betroffen sind. Auch hier werden die festgestellten Mängel kategorisiert und für die Umsetzung der Massnahmen Fristen angesetzt. Im Bereich des Gesundheitswesens konnten im Berichtsjahr verschiedene Prüfungen der Klinikinformationssysteme von Spitälern in die Wege geleitet werden. Diese Prüfungen finden zum Teil mit Unterstützung von externen Auditfirmen statt. Die Prüfungen sind noch nicht abgeschlossen.

Neben der Kontrolltätigkeit spielen die Vorabkontrollen für den präventiven Datenschutz eine wesentliche Rolle. Die öffentlichen Organe sind immer wieder auf diese Vorabkontrollpflicht hinzuweisen, denn nur wenn die Vorabkontrolle rechtzeitig erfolgt, können in einem Projekt auch vorausschauend Massnahmen zur Verringerung der Risiken getroffen werden

Bedrohungsmanagement bei der Kantonspolizei

Die Kantonspolizei informierte den Datenschutzbeauftragten über die Einführung eines neuen Datenregisters. Das neue Register soll der Geschäftskontrolle, der Ressourcenzuteilung und dem Erheben von Statistiken betreffend die Aufgabenerfüllung im präventiven Bereich dienen.

Aufgrund der Unterlagen, die dem Datenschutzbeauftragten zu diesem Zeitpunkt zur Verfügung standen, war die Rechtslage schwer einzuschätzen. Deshalb wurde eine Kontrolle vor Ort geplant und durchgeführt. Geprüft wurden die Rechtmässigkeit der Datenbearbeitungen und des Datenregisters, die Verhältnismässigkeit der Zugriffe sowie die Informationssicherheit mit Blick auf die Protokollierung.

Die Kontrolle hat ergeben, dass das Führen des Datenregisters zum Zweck der Geschäftskontrolle durch die Rechtsgrundlagen abgedeckt ist. Soweit das polizeiliche Handeln im Informationssystem POLIS dokumentiert wird und die Datenbank nur dem eingangs erwähnten Zweck dient, kann diese unter § 52 Polizeigesetz subsumiert werden.

Weiter bearbeitet die Kantonspolizei im Rahmen des Bedrohungsmanagements Daten für präventive Aufgaben, indem sie Einträge im POLIS aufgrund vorgegebener Kriterien sichtet und bei Verdacht auf Bedrohungen Massnahmen ergreift. Dies gehört zur Aufgabenerfüllung, zählen doch § 3 Abs. 2 lit. a und § 4 Polizeigesetz explizit das Verhindern und Erkennen von Straftaten auf, und ist daher aus datenschutzrechtlicher Sicht nicht zu beanstanden. Auslöser für weitere Massnahmen respektive Datenbearbeitungen sind Hinweise auf strafbare Handlungen oder mögliches strafbares Verhalten in der Zukunft.

Nicht von diesen Rechtsgrundlagen gedeckt sind jedoch Datenbearbeitungen im Rahmen des Einsatzes neuer Instrumente, welche beispielsweise automatisierte Screenings oder andere Analysen vornehmen könnten, denen keine Verdachtsfaktoren im Einzelfall zugrunde liegen und die aufgrund der automatischen Verarbeitung nachteilige Rechtsfolgen für die Betroffenen herbeiführen könnten. Nicht gedeckt sind weiter Datenbearbeitungen in Bezug auf polizeiliches Handeln betreffend Einzelfälle, die nicht im POLIS dokumentiert werden.

Einträge werden nach zehnjähriger Aufbewahrungsfrist für Gewaltschutzverfahren gemäss § 18 Abs. 5 lit. g POLIS-Verordnung sowohl in der Datenbank Bedrohungsmanagement als auch im POLIS gelöscht.

Zugriffe auf diese Datenbank sind aufgrund der Sensitivität der Daten analog den Daten im POLIS zu protokollieren.

§ 8 IDG
§ 52 Polizeigesetz
§§ 3 Abs. 2 lit. a und 4 Polizeigesetz

Elektronische Datenübermittlung an die Statthalterämter

Die Kantonspolizei plant, den Statthalterämtern die für das Übertretungsstrafverfahren notwendigen Unterlagen statt wie bisher in Papierform neu elektronisch zukommen zu lassen. Ausgenommen von diesem Prozess sollen Dokumente sein, die eine Unterschrift erfordern. Die Schnittstelle soll analog der bereits existierenden zur Staatsanwaltschaft eingerichtet werden. Heute übermittelt die Polizei bei einer Übertretung alle strafrechtlichen Unterlagen wie Polizeirapporte, Befragungsprotokolle, Fotos, Strafanträge, Verfügungen, Strafbefehle und Berichte in Papierform an die Statthalterämter. Diese erteilen der Polizei ergänzende Ermittlungsaufträge, auch dies in Papierform. Diese Art des Datenflusses ist nicht nur ineffizient, sie birgt auch Gefahren der Falscherfassung.

Die Kantonspolizei gelangte an den Datenschutzbeauftragten mit der Bitte, im Rahmen einer Vorabkontrolle zu prüfen, ob die Voraussetzungen für eine elektronische Datenübermittlung gegeben sind.

Der Datenschutzbeauftragte hat die Rechtsgrundlagen geprüft und festgestellt, dass sich die geplanten Datenflüsse mehrheitlich auf hinreichend bestimmte Rechtsgrundlagen abstützen. Einzig für die Datenflüsse im Zusammenhang mit den Strafbefehlen und Verfügungen mit sichergestellten Gegenständen liegt keine Rechtsgrundlage vor, die einen solchen Meldefluss legitimieren würde. Dies trotz der Tatsache, dass die Polizei auf die Rückmeldungen dieser Informationen angewiesen ist.

Wesentlich ist, dass kein neuer Datenaustausch und keine automatisierte Datenbearbeitung stattfinden. Auch werden keine automatisierten Abgleiche vorgenommen. Vorbehalten bleibt die Umsetzung von der Schutzstufe 3 angemessenen und in der ISV vorgeschriebenen Sicherheitsmassnahmen, welche denjenigen der Schnittstelle zur Staatsanwaltschaft entsprechen und die Vorgaben des Standards eCH-0051 2.00 erfüllen.

§ 10 IDG
§ 8 IDG
§§ 8 ff. ISV
§ 54 a PolG
Art. 312 StPO

Datensicherheit an Berufsschulen

Das Gewährleisten der Sicherheit von Daten ist und bleibt wichtig, auch an Schulen. Das IDG enthält einen zentralen Paragraphen, welcher die Schulen verpflichtet, angemessene organisatorische und technische Massnahmen zum Schutz der Informationen zu ergreifen. Welches diese angemessenen Massnahmen sind, wird in der Bestimmung nicht konkretisiert, sondern muss aus Standards abgeleitet werden. Aus einer Vielzahl von aufgelisteten Massnahmen gilt es, die je nach Sicherheitsstufe relevanten Massnahmen zu definieren. Im nächsten Schritt sind die notwendigen Dokumente, beispielsweise eine Leitlinie zur Informationssicherheit, eine Schutzbedarfsfeststellung für die Fachanwendungen oder ein Rollen- und Berechtigungskonzept zu erstellen. Zuletzt muss der Inhalt im Schulalltag umgesetzt werden. Danach sind das periodische Überprüfen von Neuerungen und die laufende Aktualisierung der Massnahmen auf den aktuellen Stand der Technik zu beachten.

Nicht alle Dokumente, die beim Umsetzen der Informationssicherheit als Grundlage dienen, müssen von jeder Schule neu erstellt werden. Teilweise können Musterdokumente erstellt, Massnahmenpläne definiert und übernommen werden. Um den Schulen die Arbeiten zum Schutz der Daten zu erleichtern, erarbeitete der Datenschutzbeauftragte zusammen mit Mitarbeitenden des Mittelschul- und Berufsbildungsamts ein umfassendes Konzept mit allen notwendigen Dokumenten analog demjenigen, das für Gemeinden bereits auf der Website verfügbar ist.

Die Dokumente umfassen einen Leitfaden Informationssicherheit, eine Leitlinie zur Informationssicherheit, eine Vorlage für eine Weisung zur Informationssicherheit, eine Erklärung über die Nutzung von Internet und E-Mail, eine Anleitung über den Aufbau und die Struktur einer Informationssicherheitsorganisation, eine Anleitung zur Sensibilisierung der Mitarbeitenden, ein Beispiel eines Rollen- und Berechtigungskonzepts, einen auf die Mittel- und Berufsschulen zugeschnittenen Massnahmenplan, ein Beispiel einer Schutzbedarfsfeststellung sowie das Inhaltsverzeichnis einer Betriebsdokumentation.

§ 7 IDG

Kleine-Weltentdecker-App

Im Rahmen seiner Forschungstätigkeit plant ein Lehrstuhl der Universität die wissenschaftliche Analyse der Entwicklungsschritte bei Kleinkindern im Alter bis sechs Jahren. Zu diesem Zweck soll interessierten Eltern ein elektronisches Entwicklungstagebuch zur Verfügung gestellt werden. Mit dieser App können sie das Wachstum und die Entwicklung ihrer Kinder in den Bereichen Sprache, Motorik, Kognition und soziale Kompetenz anhand der Beantwortung von Fragen dokumentieren. Die Antworten werden in pseudonymisierter Form an eine zentrale Plattform des Lehrstuhls übermittelt. Die Auswertungen erfolgen anonym, sodass keine Rückschlüsse auf die Kinder möglich sind. Das Vorhaben unterliegt der Vorabkontrolle durch den Datenschutzbeauftragten, da eine Vielzahl besonderer Personendaten erhoben werden. Zudem können mit diesen Informationen Persönlichkeitsprofile der Kinder erstellt werden.

Die Vorabkontrolle ergab, dass sich das Erheben der Daten durch den Lehrstuhl auf eine genügende rechtliche Grundlage abstützt. Es handelt sich um eine freiwillige Teilnahme für die Betroffenen. Sie müssen ausdrücklich über die Art der Datenbearbeitung informiert werden und in diese explizit einwilligen.

Bereits vor dem Herunterladen der App müssen die konkreten Datenbearbeitungen ersichtlich sein. Die explizite Zustimmung ist beim erstmaligen Öffnen der mobilen Applikation einzuholen. Eine weitere Zustimmung ist erforderlich, wenn die Daten zu anderen als vorgängig informierten Zwecken bearbeitet werden. Die organisatorisch-rechtlichen Anforderungen richten sich nach IDG und ISV. Nebst den Anforderungen des IT-Grundschutzes müssen auch Vorgaben an die App selber umgesetzt werden, wie sie zum Beispiel im Mobile Security Project des Open Web Application Security Project (OWASP) definiert sind.

§ 2 Abs. 1 i.V.m. § 24 Universitätsgesetz
§ 3 Abs. 4 IDG
§ 10 IDG i.V.m. § 24 Abs. 1 lit. b IDV
§ 12 IDG

Kontrolle der Massnahmenumsetzung in einer Gemeinde

Gestützt auf den gesetzlichen Auftrag kontrollierte der Datenschutzbeauftragte im Jahr 2014 eine mittelgrosse Zürcher Gemeinde in den Bereichen Recht, Organisation und Technik. Bei der Kontrolle wurden im rechtlichen Bereich Mängel bezüglich Zugriffen anderer öffentlicher Organe, Vertragsverhältnisse sowie Aufbewahrungsfristen entdeckt. Technisch zeigten sich Mängel bei den Vorgaben und dem Betrieb in Bezug auf die Informationssicherheit, die interne und externe Stellen betraf, sowie bei der Schulung und der Regelung der Zugriffsberechtigungen.

Der Datenschutzbeauftragte verlangte in seinem Kontrollbericht die Umsetzung verschiedener Massnahmen. Eine Nachkontrolle bei der Gemeinde 2016 ergab, dass die Zugriffe in der Zwischenzeit durch einen Gemeinderatsbeschluss geregelt und ein Dienstleistungsvertrag erstellt worden waren. Die technischen Massnahmen waren hingegen noch nicht vollständig umgesetzt. Vor allem in den Bereichen Informationssicherheitsmanagement, Betreiberweisungen sowie Regelungen bezüglich mobilen Geräten und Passwörtern bestand noch Handlungsbedarf. Der Rückstand konnte einerseits durch einen Wechsel zu einem neuen IT-Dienstleistungsanbieter und den entsprechenden Umstellungen erklärt werden. Andererseits verzögerte der Umzug eines Rechenzentrums des Auftragnehmenden die Erstellung verschiedener Dokumente.

Festzustellen war aber, dass sich die Gemeinde der Umsetzung der Massnahmen engagiert angenommen hat und diese weiterverfolgt. Der Datenschutzbeauftragte wird über die weiteren Entwicklungen auf dem Laufenden gehalten.

Kontrolle der Massnahmenumsetzung in einem Spital

Der Datenschutzbeauftragte hatte 2015 im Rahmen seines gesetzlichen Auftrags in einem Spital einen Datenschutzreview durchgeführt und die Umsetzung der rechtlichen, organisatorischen und technischen Anforderungen an die Datenbearbeitungen geprüft. Die Prüfung im rechtlichen Bereich zeigte Verbesserungspotenzial bei den Verträgen über die Auslagerung von Datenbearbeitungen sowie bei den Aufbewahrungsfristen für Papier- und elektronische Akten. Im technischen Bereich fielen vor allem das Fehlen einer Leitlinie und eines Informationssicherheitsmanagementsystems (ISMS) sowie Mängel im IT-Sicherheitskonzept auf. Zudem fehlten ein übergreifendes Rollen- und Berechtigungskonzept, eine Planung für Sensibilisierungsmassnahmen, Weisungen für den Betreibenden und eine Regelung der Verantwortlichkeiten.
Im Jahr 2016 kontrollierte der Datenschutzbeauftragte die Umsetzung der Massnahmen zur Verbesserung der Informationssicherheit.

Die Spitalleitung hatte auf den Bericht zum Datenschutzreview mit der Beauftragung einer in IT-Sicherheitsfragen spezialisierten Beratungsfirma reagiert und ein Projekt mit vier Leistungspaketen (Leitlinien Framework, Risikomanagementprozess, Rollen- und Berechtigungskonzept, Sensibilisierung) zur ganzheitlichen Umsetzung der Massnahmen nach dem Top-Down-Prinzip und in drei Phasen (Konzeption, Implementierung und Betrieb) erstellt. Die Fertigstellung der letzten Phase war bis Ende 2018 vorgesehen. Das Projekt beinhaltete optional eine Zertifizierung des ISMS nach ISO 27001. Die Kontrolle der Massnahmenumsetzung ergab, dass aufgrund von personellen Wechseln sowie anderen Faktoren Verzögerungen im Terminplan aufgetreten sind. Der Datenschutzbeauftragte wird vom Spital über den Stand der Umsetzung auf dem Laufenden gehalten.

«Youtuberinnen und Youtuber setzen verschiedene Aspekte des Datenschutzes visuell um und bearbeiten Themen, die sie für ihren Alltag als relevant betrachten, in der Art und Form, die von ihrer Gemeinschaft verstanden wird.»

Informations- und Weiterbildungsangebote

Die Zunahme der Weiterbildungsangebote für öffentliche Organe um mehr als einen Drittel zeigt das Bedürfnis nach einschlägigen Informationen zu Datenschutz und Sicherheit. Insbesondere Kurse und Seminare sind sehr aufwendig, weshalb die bestehenden Kapazitäten des Datenschutzbeauftragten hier Grenzen setzen. Aufgrund der Zusammenarbeit mit dem Zürcher Zentrum für Informationstechnologie und Datenschutz der ZHAW kann ein Teil der Kurse extern durchgeführt werden.

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
2016	28

Zunehmend wird das Bedürfnis nach spezifischen Informationen auch durch den Ausbau des Informationsangebots des Datenschutzbeauftragten aufgefangen. So enthält die Website immer mehr vertiefte Informationen zu einzelnen Bereichen, die in sogenannten Lexika zusammengefasst sind. Im Berichtsjahr konnte das Datenschutzlexikon Volksschule aufgeschaltet werden. Zusätzlich ist das Lexikon in die Datenschutz.ch-App integriert und so auch für die mobilen Nutzerinnen und Nutzer ständig verfügbar.

Das Datenschutzlexikon Volksschule ist auf ein sehr breites und positives Echo gestossen. Deshalb wurde dieses Konzept im Berichtsjahr weitergeführt mit Projekten für ein Datenschutzlexikon Hochschule und ein Datenschutzlexikon Einwohnerkontrolle, welche beide in der Zwischenzeit online zur Verfügung stehen.

Um bestimmte Zielgruppen erreichen zu können, spielen die sozialen Medien eine immer wichtigere Rolle. Jugendliche lassen sich über Youtube direkt ansprechen, weshalb dieser Kanal im Berichtsjahr weiter ausgebaut wurde. Ebenso informiert der Datenschutzbeauftragte mittels Twitter über Neuigkeiten und weist auf Kurse und Seminare hin.

Seminare und Kursmodule

– Datenschutz – Herausforderung Digitalisierung
– Seminar Datenschutz im Sozialbereich
– Seminar Datenschutz im Gesundheitswesen
– Internes Seminar für Mitarbeitende im Kinder- und Jugendbereich
– Workshop «Die digitale Welt und der Zauber des Privaten»
– Informationssicherheit – Datenschutz – Öffentlichkeitsprinzip (Gemeindefachschule, KV Zürich Business School)
– CAS Clinical Trial Management (USZ)
– CAS Kinder- und Erwachsenenschutzrecht (ZHAW)

Ausgewählte Referate

– Aktuelle Herausforderungen des Datenschutzrechts
– Datenschutz im europäischen Rechtsraum
– Big Data im Bereich Sozialversicherung
– Digitale Gesellschaft – das Freiheitsparadox und die Rolle des Datenschutzes
– Schutz und Sicherheit im Internet
– Welchen Datenschutz braucht die Schweiz?
– E-Government – Datenschutz als Risiko?

Kluges Verhalten in den sozialen Medien

Soziale Medien haben den Umgang mit persönlichen Daten verändert. Immer mehr Privates wird bekannt gegeben. Deshalb lässt der Datenschutzbeauftragte Youtuberinnen und Youtuber zu Wort kommen, um in ihrer Sprache Antworten auf die Frage «Why privacy matters» zu finden.

Jugendliche und junge Erwachsene informieren sich bevorzugt über Online-Videos. Deshalb hat der Datenschutzbeauftragte verschiedene Projekte lanciert, um über die Videoplattform Youtube in Sachen Datenschutz und Schutz der Persönlichkeit zu sensibilisieren. Unter dem Titel «Why privacy matters» respektive «Warum braucht es Datenschutz» setzen Youtuberinnen und Youtuber verschiedene Aspekte des Datenschutzes visuell um. Sie bearbeiten diejenigen Themen, die sie für ihren Alltag als relevant betrachten, in der Art und Form, die ihre Gemeinschaft versteht. Verschiedene Faktoren machen diesen Peer-to-Peer-Ansatz zu einem Erfolgsrezept:

– Digital Natives werden selbst aktiv und integrieren die Themen des Datenschutzes in ihr Schaffen.
– Die relevanten Themen werden für ihre Community aufgearbeitet und die Botschaften bekommen dadurch eine erhöhte Glaubwürdigkeit.
– Die Botschaften werden breit gestreut.
– Die Arbeiten geben Indizien über das vorhandene Wissen.

Wettbewerb zum Europäischen Datenschutztag

Mit einem Videoaufruf gab der Datenschutzbeauftragte am Europäischen Datenschutztag 2016 den Startschuss für einen Wettbewerb, für den die Youtube-Gemeinschaft Videos zum Thema Datenschutz und Schutz der Privatsphäre einreichen konnte. Beurteilt wurden die Videos von einer Jury, der neben dem Datenschutzbeauftragten auch Youtuberinnen und Fachpersonen der Sparte audiovisuelle Medien sowie Literatur- und Medienwissenschaften angehörten. Sie orientierte sich an den Kriterien Inhalt, Handwerk und Originalität. Als Preise waren Produktionsbeiträge ausgesetzt.

Die eingegangenen Videos überzeugten durch die Vielfalt, wie die Themen bearbeitet wurden, und die hohe handwerkliche und inhaltliche Qualität. Das Gewinnervideo ist ein Trickfilm, der auf radikal-einfache Art und Weise die Wichtigkeit des technischen Datenschutzes veranschaulicht, während der zweitplatzierte Clip praktische Tipps und Tricks für einen besseren Datenschutz gibt. Der drittplatzierte Beitrag thematisiert auf sehr eingängige und witzige Weise die Herausforderungen des Schutzes der Privatsphäre angesichts der Allgegenwärtigkeit von Smartphones in unserem Alltag.

Auf dem Youtube-Kanal des Datenschutzbeauftragten wird der Schutz der Privatheit direkt in den sozialen Netzwerken diskutiert und gefördert.

Ein Lexikon für die Volksschule

Im Jahr 2016 veröffentlichte der Datenschutzbeauftragte sein erstes Datenschutzlexikon. Das handliche Nachschlagwerk wird periodisch aktualisiert und gibt Angehörigen der Volksschulen sowie Eltern und Lernenden Antworten und Sicherheit.

Im Schulalltag sehen sich Lehrpersonen, Mitglieder von Schulleitungen, Mitarbeitende des schulpsychologischen Dienstes und andere Fachleute, aber auch Eltern und Schülerinnen und Schüler einer Vielfalt datenschutzrechtlicher Herausforderungen gegenüber. Das zeigt sich in der grossen Anzahl Beratungsanfragen an den Datenschutzbeauftragten.

Mit dem umfassenden und praxisnahen Datenschutzlexikon für Volksschulen werden die häufigsten Fragen schnell und unkompliziert beantwortet. Zu diesem Zweck wertete der Datenschutzbeauftragte die Beratungsanfragen der letzten Jahre aus und ordnete die Antworten Schlagwörtern aus dem schulischen Alltag zu. So entstand ein alphabetisches Verzeichnis, das einen Überblick der Bandbreite aller datenschutzrechtlichen Fragen an Volksschulen gibt. Die Antworten umfassen neben kurzen und konkreten Erklärungen zur rechtlichen Situation auch zahlreiche Hinweise auf weiterführende Informationen des Datenschutzbeauftragten oder anderer Institutionen.

An Volksschulen arbeiten Mitarbeitende geografisch weit verstreut, sehr flexibel und oft ohne festen Arbeitsplatz. Diesen Herausforderungen muss auch bei der Aufbereitung der Informationen Rechnung getragen werden. Deshalb lag es auf der Hand, die Inhalte des Datenschutzlexikons nicht nur in PDFs, sondern auch über eine App zugänglich zu machen, denn das Smartphone ist jederzeit dabei und mit der App des Datenschutzbeauftragten sind so auch die Antworten auf mögliche Fragen immer zur Hand.

Die zahlreichen positiven Reaktionen auf die Lancierung des Datenschutzlexikons sowie die grosse Anzahl heruntergeladener Apps machte offenkundig, dass das neue Angebot einem Bedürfnis entsprach. Fachmedien verbreiteten die Information über das neue Angebot und in Referaten an Pädagogischen Hochschulen und vor IT- und Lehrpersonengremien konnte der Datenschutzbeauftragte die Sensibilisierung für schulische Aspekte des Datenschutzes fördern. «Die Schlagwörter machten mir erst klar, welche Aspekte zu berücksichtigen sind», war die Reaktion einer Lehrperson.

Das Datenschutzlexikon ist auf der Website www.datenschutz.ch als PDF verfügbar und ist Teil der Datenschutz.ch-App, die für iOS und Android kostenlos heruntergeladen werden kann. Bleibt eine Frage unbeantwortet, bietet die App die Möglichkeit, direkt mit dem Datenschutzbeauftragten Kontakt aufzunehmen.

«Die Erhebung der Fernmeldekontaktdaten diente nicht der Überprüfung des Tatverdachts gegen eine bestimmte Person, sondern versuchte diesen erst zu begründen. Ein hinreichender Tatverdacht bestand nicht.»

Bundesgericht bestätigt Ergebnisse der Kontrolle betreffend Universität

Die Universität Zürich (UZH) hatte im September 2012 Strafanzeige wegen Verdachts der Amtsgeheimnisverletzung erstattet, nachdem in den Medien Berichte betreffend das Medizinhistorische Institut und Museum der UZH veröffentlicht worden waren. Im Herbst 2013 war bekannt geworden, dass die UZH der Staatsanwaltschaft verschiedene Daten von Angehörigen der UZH sowie von Dritten herausgegeben hatte und dazu eine unbekannte Menge an Telefon- und E-Mail-Daten auf bestimmte Kontakte hin überprüft worden waren. Der Datenschutzbeauftragte hatte darauf bei der UZH eine Kontrolle eingeleitet, um die Rechtmässigkeit dieser Datenbearbeitungen zu prüfen. Die Kontrolle hatte ergeben, dass die UZH unrechtmässig Telefon- und E-Mail-Verkehrsdaten ausgewertet und an die Staatsanwaltschaft herausgegeben hatte (Tätigkeitsbericht 2014, Seite 12). Der Bericht der Kontrolle ist auf www.datenschutz.ch abrufbar. Das Bundesgericht kommt in einem Urteil in dieser Sache zum selben Ergebnis.

Anlass für den Bundesgerichtsentscheid war das in diesem Zusammenhang durchgeführte Strafverfahren, in dem das Bezirksgericht Zürich die Angeklagte freisprach. Es begründete den Freispruch damit, dass die wesentlichen Beweismittel, auf welche sich die Anklage stützte, nicht verwertbar seien. Das Obergericht, bei dem Berufung eingelegt worden war, kam zum gleichen Ergebnis. Das Bundesgericht als letzte Beschwerdeinstanz bestätigte diese Urteile mit den folgenden Argumenten.

Da es sich bei der UZH nicht um eine Privatperson, sondern um eine kantonale Behörde im Sinn von Art. 194 Abs. 2 i.V.m. Art. 44 StPO handelt, konnte die Staatsanwaltschaft diese weder im Sinne von Art. 265 Abs. 3 StPO hoheitlich zur Herausgabe der gewünschten Fernmeldedaten auffordern noch hätte sie sie in Anwendung von Art. 263 StPO beschlagnahmen können, falls die Behörde die Herausgabe verweigert hätte. Vielmehr wäre die UZH unter bestimmten Voraussetzungen zur Rechtshilfe verpflichtet gewesen. Gemäss Art. 194 Abs. 2 StPO stellen Verwaltungs- und Gerichtsbehörden den Strafbehörden ihre Akten zur Einsichtnahme zur Verfügung, wenn der Herausgabe keine überwiegenden öffentlichen oder privaten Geheimhaltungsinteressen entgegenstehen. Weil sich die Staatsanwaltschaft für die verschiedenen Begehren an die UZH um Auswertung und Zustellung von Fernmeldekontaktdaten nie ausdrücklich auf Art. 194 Abs. 2 StPO stützte und namentlich keine als solche bezeichneten, förmlichen Rechtshilfebegehren an die angefragten Behörden richtete, war unklar, ob den seitens der UZH handelnden Personen bewusst war, dass die Herausgabe der Fernmeldekontaktdaten an die Staatsanwaltschaft auf dem Weg der Rechtshilfe zu geschehen hatte und hätte verweigert werden können. Die Beweiserhebung ist nur als rechtmässig einzustufen, soweit im Zusammenwirken der Staatsanwaltschaft und der UZH die Grundsätze rechtsstaatlichen Handelns gemäss Art. 5 BV eingehalten und die Grundrechte der betroffenen Personen ausreichend beachtet wurden.

Für die Angehörigen und Mitarbeitenden der UZH war die Auswertung der Fernmeldedaten nach den Vorgaben der Staatsanwaltschaft mit einem Eingriff gemäss Art. 13 Abs. 1 BV verbunden, zumal ihnen der private Gebrauch von Telefon und E-Mail in gewissem Umfang ausdrücklich erlaubt war und sie nicht mit einer personenbezogenen Auswertung ihrer Fern-

meldekontaktdaten rechnen mussten. Verfahrenshandlungen der Strafbehörden, die in Grundrechte der Betroffenen eingreifen und dazu dienen, Beweise zu sichern, gelten als Zwangsmassnahmen (Art. 196 lit. a StPO). Der mit der Auswertung und Erhebung der Fernmeldedaten verbundene Eingriff in das von Art. 13 Abs. 1 BV geschützte Fernmeldegeheimnis ist nur zulässig, wenn ein hinreichendes öffentliches Interesse besteht und er verhältnismässig ist. Diese verfassungsmässigen Voraussetzungen der Einschränkung von Freiheitsrechten werden für die strafprozessualen Zwangsmassnahmen in dem Sinn konkretisiert, dass sie einen hinreichenden Tatverdacht voraussetzen.

Die Staatsanwaltschaft konnte zwar vermuten, dass eine allfällige Täterschaft der UZH zuzuordnen sei. Der Tatverdacht konnte zum Zeitpunkt der Erhebung der Kontaktdaten jedoch noch keiner Person zugeordnet werden. Die Auswertung der Fernmeldedaten wurde denn auch nicht auf bestimmte Personen eingeschränkt, die – im Vergleich zu anderen Mitarbeiterinnen und Mitarbeitern der UZH – eher als Täterschaft in Frage kamen. Vielmehr wurde eine flächendeckende nachträgliche Überprüfung der Festnetz- und Mobiltelefonanschlüsse und E-Mail-Konten sämtlicher Angehöriger und Mitarbeitenden der Universität durchgeführt. Die Erhebung der Fernmeldekontaktdaten diente somit nicht der Überprüfung des Tatverdachts gegen eine bestimmte Person oder bestimmte Personen, sondern versuchte diesen erst zu begründen. Ein hinreichender Tatverdacht im Sinn von Art. 197 Abs. 1 lit. b StPO, welcher die Erhebung der Fernmeldedaten gerechtfertigt hätte, bestand somit nicht.

Das Bundesgericht kam zum Ergebnis, dass die Fernmeldekontaktdaten ohne Vorliegen eines hinreichenden Tatverdachts sowie in unverhältnismässiger Art und Weise und somit in Verletzung von Art. 197 Abs. 1 und 2 StPO erhoben worden waren, womit sie in Anwendung von Art. 141 Abs. 2 StPO nicht verwertbar sind.

Urteil des Bundesgerichts 1B_26/2016 vom 29. November 2016

Rechtsgrundlagen für Kontrolle und Einsatz von Trojanern

Im Sommer 2015 wurde bekannt, dass die Kantonspolizei Spionagesoftware (sogenannte Government Software, GovWare, auch Staatstrojaner genannt) einsetzt. Dies nachdem der ausländische Lieferant der Software gehackt worden war und Unterlagen über die Beschaffung an die Öffentlichkeit gelangten. Der Datenschutzbeauftragte verlangte daraufhin, dass die GovWare zur Vorabkontrolle vorgelegt wird, was die Kantonspolizei ablehnte (Tätigkeitsbericht 2015, Seiten 10 und 11). In der Folge gelangte er an die Sicherheitsdirektion und schlug eine Aussprache vor.

Auch die Geschäftsprüfungskommission des Kantonsrats (GPK) befasste sich mit der Angelegenheit und setzte dazu eine Subkommission ein.
Ihr Bericht vom 19. Mai 2016 (KR-Nr. 166/2016) wurde im Kantonsrat am 20. Juni 2016 diskutiert. In Bezug auf die rechtlichen Fragen, ob die Beschaffung und der Einsatz von GovWare rechtmässig sind und ob die GovWare der Vorabkontrolle untersteht, nahm der Bericht keine abschliessende Beurteilung vor. Die GPK erachtete jedoch eine Aussprache zwischen dem Datenschutzbeauftragten und der Sicherheitsdirektion als zielführend. Damit bestätigte sie das vom Datenschutzbeauftragten gewählte Vorgehen. Diese Aussprache ist noch offen.

Die GPK hatte in ihrem Bericht den fehlenden Einbezug des Datenschutzbeauftragten bei der Beschaffung und dem Einsatz von neuen Technologien wie GovWare festgestellt. In der Folge erteilte die Geschäftsleitung des Kantonsrates der GPK den Auftrag, die Anwendung des Informations- und Datenschutzgesetzes (IDG) in den Direktionen näher zu überprüfen (Tätigkeitsbericht der GPK vom 2. März 2017, Seite 40; KR-Nr. 62/2017).

Zwischenzeitlich haben die Eidgenössischen Räte die Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) beschlossen (Bundesblatt 2016, Seite 1991 ff.). Im Rahmen dieser Revision wird auch die Strafprozessordnung geändert. Sie wird künftig Rechtsgrundlagen für den Einsatz von GovWare enthalten. Ebenso wird aufgrund der Anpassungen des IDG an europarechtliche Vorgaben die Pflicht zur Vorabkontrolle klar geregelt werden (Seiten 6 und 7).

Impressum

Herausgeber: Datenschutzbeauftragter des Kantons Zürich, Postfach, CH-8090 Zürich
Korrektorat: Text Control, Im Struppen 11, 8048 Zürich
Layout: René Habermacher, Visuelle Gestaltung, Artherstrasse 25, 6405 Immensee

Der Tätigkeitsbericht 2016 ist elektronisch verfügbar unter www.datenschutz.ch/TB2016.

Kontakt

E-Mail datenschutz@dsb.zh.ch
Internet www.datenschutz.ch
Twitter https://twitter.com/dsb_zh
Youtube www.youtube.com/channel/UCghVVLU_hOTbCIYaKQk8hTw
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