dsb

datenschutzbeauftragter
kanton zürich

Tätigkeitsbericht 2017

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 2017 bis und mit 31. Dezember 2017 ab und ist im Internet unter www.datenschutz.ch veröffentlicht.

Zürich, im April 2018

Der Datenschutzbeauftragte des Kantons Zürich

Dr. Bruno Baeriswyl

Datenschutz-beauftragter 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 (Datenschutzreviews), 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

Überblick

Eine digitale Zukunft mit Datenschutz

Die fortschreitende Digitalisierung ist der dominierende Treiber der Datenbearbeitungen der Verwaltung. Bei den zahlreichen Projekten sind die grundsätzlichen Fragen des Datenschutzes und der Sicherheit nicht durchwegs berücksichtigt.

Datenbearbeitungen des Staates müssen sich an die Vorgaben des demokratischen Rechtsstaats halten. In der Hektik der technologischen Entwicklung und angesichts der verführerischen Attraktivität der neuen Möglichkeiten geht oft vergessen, dass staatliches Handeln immer auf einer Rechtsgrundlage beruhen muss, welche die Verhältnismässigkeit und das öffentliche Interesse berücksichtigt. Dies gilt ganz grundsätzlich und deshalb auch bei Eingriffen in die persönliche Freiheit der Bürgerinnen und Bürger, also beim Datenschutz.

Persönliche Freiheit schützen

Digitalisierungsprojekte öffentlicher Organe können nicht an die Einwilligung der Betroffenen geknüpft oder durch ein überwiegendes öffentliches Interesse gerechtfertigt werden.

Der Datenschutzbeauftragte muss immer wieder darauf hinweisen, dass auch in der Digitalisierung die Grundlagen des demokratischen Rechtsstaates zu beachten sind und staatliches Datenbearbeiten auf einer demokratisch legitimierten Rechtsgrundlage zu erfolgen hat.

Der Datenschutz ist ein Grundrecht und keine Materie, die nach Belieben ausgelegt werden kann. Selbstverständlich findet bei jeder Gesetzgebung eine Interessenabwägung zwischen den Grundrechten statt. Wenn aber der Datenschutz zur Disposition gestellt oder gar ein Zielkonflikt zwischen Digitalisierung und Datenschutz heraufbeschworen wird, dann werden gleichzeitig die Freiheitsrechte der Bürgerinnen und Bürger in Frage gestellt. Diese zu wahren, muss jedoch ein Ziel der Digitalisierung sein.

Datenvermeidung und Datensparsamkeit

Jede Nutzung von elektronischen Kommunikationsmitteln gibt Auskunft über das Wann, Wo und Wie der Kommunikation und somit über das Verhalten einer Person. Über eine längere Zeitperiode entstehen damit Persönlichkeitsprofile, die ein erhöhtes Risiko für eine Grundrechtsverletzung beinhalten. Mit der Digitalisierung müssen deshalb auch Strategien zur Datenvermeidung und Datensparsamkeit umgesetzt werden.

Hierzu dient die generelle Technologiefolgenabschätzung, welche die Chancen und Risiken aufzeigt und aufgrund der die Risiken durch geeignete Massnahmen reduziert werden können. Wer nur von Effizienz und Wirkung spricht, verkennt, dass das Vertrauen der Bürgerinnen und Bürger in den Schutz und die Sicherheit ihrer Daten ebenso wichtig ist.

Cloud Computing als Herausforderung

Das Cloud Computing ist zurzeit das am breitesten genutzte Angebot der neuen Technologien. Meist grosse Anbieter stellen dafür riesige Infrastrukturen zur Verfügung, die jede Art von Datenbearbeitungen ermöglichen, ohne dass Nutzende eigene Hard- oder Software im grossen Stil betreiben müssen. Auch für diese Auslagerung gelten die datenschutzrechtlichen Vorgaben und müssen die entsprechenden Sicherheitsanforderungen erfüllt werden. Im Fokus standen beim Datenschutzbeauftragten Fragen des Schutzes des Berufsgeheimnisses im Gesundheitsbereich (Arzt- oder Patientinnengeheimnis, Seite 18) und der rechtlichen Rahmenbedingungen für Cloud-Lösungen auf den verschiedenen Schulstufen (Seite 19). Bei der Sicherheit waren insbesondere Anforderungen an die Verschlüsselungslösungen zu diskutieren (Seite 21).

Kontrolle von Outsourcingnehmer

Zum ersten Mal kontrollierte der Datenschutzbeauftragte auch einen Outsourcingnehmer, der für zahlreiche Gemeinden Dienstleistungen erbringt (Seite 42). Die Resultate sind erfreulich und zeigen, dass der Anbieter die Anforderungen des Datenschutzes und der Sicherheit sehr gut erfüllt. Mit diesem Ergebnis sind auch die vielen Gemeinden, die Dienstleistungen dieses Outsourcingnehmers beziehen, grundsätzlich auf der sicheren Seite. Der Datenschutzbeauftragte wird weitere Outsourcingnehmer kontrollieren.

Ausgezeichnete Bewertung

Im vergangenen Jahr hat das Statistische Amt eine Umfrage über die Zufriedenheit der Kundinnen und Kunden des Datenschutzbeauftragten durchgeführt. Dabei zeigte sich, dass eine grosse Mehrheit der Befragten mit den Leistungen des Teams des Datenschutzbeauftragten sehr zufrieden ist. Besonders zufrieden zeigten sich Angehörige der kantonalen Verwaltung sowie der Gemeinden. (Seite 11)

Zertifiziert nach ISO 9001:2015

Der Datenschutzbeauftragte ist seit 2003 nach der Qualitätsnorm ISO 9001 zertifiziert. Damit gewährleistet er einen effizienten und wirkungsorientierten Datenschutz in einer Zeit, in der die Ressourcen knapp sind und die Aufgaben auch aufgrund der beschleunigten Digitalisierung anspruchsvoller werden. Die Norm wurde durch eine neue Version ISO 9001:2015 abgelöst, was verschiedene Anpassungen am Qualitätsmanagementsystem (QMS) des Datenschutzbeauftragten nach sich zog. Diese konnten im vergangenen Jahr abgeschlossen werden und die Organisation des Datenschutzbeauftragten konnte 2018 rezertifiziert werden.

Gesetzesevaluation zeigt Handlungsbedarf

Die Evaluation der Wirkungen des IDG startete 2012 und wurde im Sommer 2017 mit einer Auswertung und einer Synthese der Teilevaluationen abgeschlossen. Die Gesetzesevaluation zeigt, dass die Bevölkerung des Kantons Zürich den Zugang zu Informationen und den Datenschutz sehr wichtig findet. In einer repräsentativen Umfrage bewerteten die Befragten die Wichtigkeit des Öffentlichkeitsprinzips und des Datenschutzes mit 7,7 respektive 8,4 von 10 Punkten. Das Wissen über das Öffentlichkeitsprinzip ist jedoch wesentlich geringer als beim Datenschutz.

Der Zugang zu Informationen ist laut dem Synthesebericht im Kanton Zürich «vergleichsweise wenig vorteilhaft» organisiert. Während der Datenschutzbeauftragte in seinem Bereich für die Bevölkerung und alle öffentlichen Organe tätig ist, gibt es für Anliegen zum Zugang zu Informationen keine zentrale Anlaufstelle, die berät, informiert und vermittelt. Bei Rekursen sehen sich die Bürgerinnen und Bürger je nach Amt verschiedenen Instanzen gegenüber, was im Synthesebericht als «unter Umständen abschreckend» bezeichnet wird. Zudem stufen die öffentlichen Organe den voraussetzungslosen Zugang zu Informationen – mit einem Durchschnittswert zwischen 5 und 6,7 – im Gegensatz zur Bevölkerung als weniger wichtig ein.

Rund sechs von zehn Personen wissen, dass es im Kanton eine Behörde gibt, an die man sich bei Datenschutzproblemen wenden kann. Die hohe Bekanntheit des Datenschutzbeauftragten macht plausibel, dass seine Informationen in der breiten Öffentlichkeit wahrgenommen werden und zur hohen Sensibilisierung beitragen.

Die Kontrolltätigkeit und die Beratungs- sowie Weiterbildungsaktivitäten des Datenschutzbeauftragten tragen zu einer gesteigerten Datenschutzsensibilität und somit zur rechtmässigen Bearbeitung von Personendaten bei. Die Wirkung der Kontrollen ist jedoch eingeschränkt, weil die betroffenen Organe viele Verbesserungshinweise nicht umsetzen und der Datenschutzbeauftragte über zu wenige Ressourcen verfügt, um die Anzahl Kontrollen durchzuführen, die im Konsolidierten Entwicklungs- und Finanzplan (KEF) vorgesehen sind.

Die Wirkung des Gesetzes verstärken

Angesichts der Erwartungshaltung, aber auch des Wissensdefizits der Bevölkerung besteht Handlungsbedarf. Das Öffentlichkeitsprinzip und die Bestimmungen zur Transparenz der Verwaltung sind kein Selbstzweck. Der niederschwellige Zugang zu Information ist vielmehr ein Instrument zur Förderung der freien Meinungsbildung, der Wahrnehmung der demokratischen Rechte und der politischen Partizipation. Die Ergebnisse der Gesetzesevaluation zeigen, dass auch der Datenschutz gestärkt werden muss. Die Bevölkerung erwartet einen zuverlässigen Schutz ihrer Daten, andererseits verstärkt die Digitalisierung die Risiken bei den Datenbearbeitungen. Die datenschutzrechtlichen Instrumente müssen deshalb durch gesetzgeberische Massnahmen angepasst werden.

Gemäss Evaluationssynthese sollte das Ziel einer Revision des IDG sein, die Sensibilität der Bevölkerung für die Datenbearbeitungen des Kantons weiter zu steigern. Die öffentlichen Organe sollen verpflichtet werden, aktiv über das Recht auf Zugang zu Informationen zu informieren. Vergleichbar mit dem Datenschutzbeauftragten soll eine unabhängige Stelle geschaffen werden, die einen Informations- und Beratungsauftrag über das Öffentlichkeitsprinzip, aber auch eine Vermittlungsfunktion gegenüber der Bevölkerung ausübt.

Weiter zeigt die Evaluationssynthese bei den Informationspflichten der öffentlichen Organe Handlungsbedarf auf und regt an, sie zu verpflichten, die betroffenen Personen bei der Beschaffung und der Weitergabe nicht nur von besonderen Personendaten, sondern von allen Personendaten aktiv zu informieren. Zudem soll der Katalog der besonderen Personendaten in Zukunft Daten zum Sexualleben, zur sexuellen Orientierung, genetische Daten und biometrische Daten sowie das Profiling umfassen. Öffentliche Organe, die besondere Personendaten bearbeiten, sollen verpflichtet werden, ihre formellen Gesetze zu prüfen, ob sie dem IDG und dem übergeordneten Recht entsprechen.

Weiter soll der Datenschutzbeauftragte gestärkt werden, indem die kantonalen Verwaltungsbehörden gesetzlich verpflichtet werden, ihn von sich aus über alle eigenen Gesetzgebungsprojekte sowie Vernehmlassungsverfahren zu Bundesvorhaben zu informieren. Der Datenschutzbeauftragte soll Verfügungskompetenz erhalten.

Aus dem Synthesebericht der Evaluation geht hervor, dass die politischen Behörden eine Erhöhung der personellen Ressourcen des Datenschutzbeauftragten prüfen sollen, da dies ihr einziges Steuerungsmittel in diesem Bereich ist. Damit käme man auch den kontrollierten öffentlichen Organen entgegen, welche die Umsetzung der Massnahmen teils als aufwendig bezeichnen und sich mehr Unterstützung wünschen.

Der Datenschutzbeauftragte setzt Empfehlungen um

2017 begann der Datenschutzbeauftragte, Empfehlungen aus der Evaluationssynthese umzusetzen. So führt er nur noch so viele Kontrollen durch, als seine Ressourcen auch für Nachkontrollen und die notwendige Unterstützung bei der Umsetzung seiner Hinweise genügen. Gleichzeitig hat er die Kontrollen neu konzipiert, um die Wirksamkeit weiter zu erhöhen. Zudem nahm er Projekte in Angriff, mit denen die Informationsanstrengungen optimiert werden können.

Die Evaluationssynthese wurde dem Regierungsrat im Hinblick auf die Revision des IDG zur Kenntnis gebracht. Das Konzept, die Berichte der Teilprojekte und der Synthesebericht der Evaluation des IDG sind auf der Website des Datenschutzbeauftragten verfügbar.

Sehr gute Noten für den Datenschutz-beauftragten

Die Personen, die mit dem Datenschutzbeauftragten Kontakt haben, beurteilen seine Leistungen überwiegend als sehr gut, wie die Resultate der Kundschaftsbefragung 2017 zeigen.

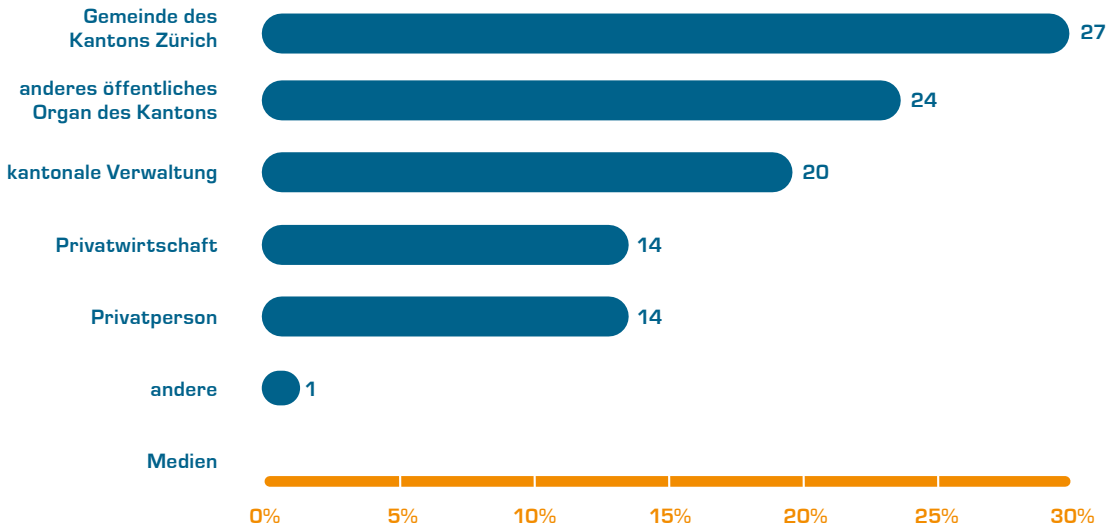
Die Zufriedenheit stieg im Vergleich zu den hohen Werten vor fünf Jahren weiter an – von 4,9 auf 5,2 von maximal 6 Punkten. Vertreterinnen und Vertreter der Verwaltung, der Gemeinden und anderer öffentlicher Organe bewerten die Dienstleistungen insgesamt mit 5,3 Punkten als sehr gut, die Kurse werden von den Teilnehmenden sogar mit 5,5 Punkten benotet. Besonders gut schnitt die telefonische Beratung mit 5,6 Punkten ab. Alle Zielgruppen schätzen insbesondere die Fachkompetenz und die Freundlichkeit und bewerten sie mit 5,3 beziehungsweise 5,5 Punkten.

In den individuellen Kommentaren verbinden die Kundinnen und Kunden die Leistungen des Datenschutzbeauftragten mit Begriffen wie Verlässlichkeit, Speditivität, Sachlichkeit und Dienstleistungsorientierung und erwähnen die offene Haltung für neue Fragestellungen. Sie schätzen die konkreten Antworten und die konstruktiven Vorschläge. Hervorgehoben wird zudem die Qualität des Informationsangebots auf der Website: von Vorlagen über Checklisten bis hin zu den Datenschutzlexika. Kurse werden von Teilnehmenden als ausgezeichnet beurteilt. Ebenfalls wird die Medienpräsenz positiv erwähnt.

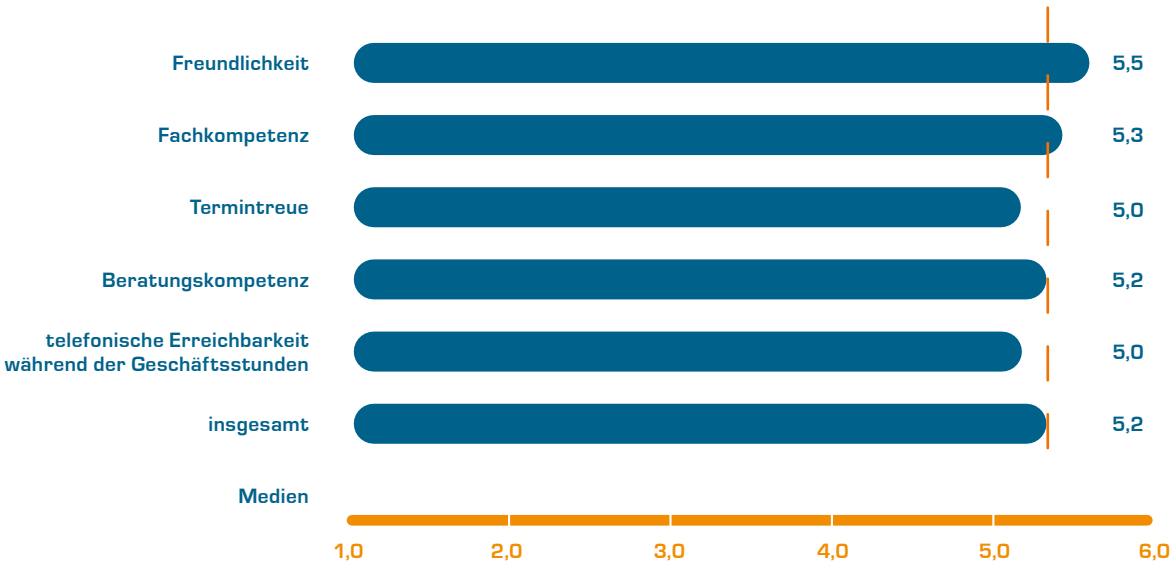
Seit der letzten Befragung vor fünf Jahren zeigt sich eine signifikante Stärkung des Bewusstseins für den Datenschutz. Beinahe 90 Prozent der teilnehmenden Kundinnen und Kunden denken, dass dem Datenschutz in ihrem Arbeitsumfeld ein hoher Stellenwert zukommt. Allerdings gehen nur knapp zwei Drittel der Befragten davon aus, dass die Personendaten immer korrekt verwendet werden.

Für die Befragung schrieb das Statistische Amt im Auftrag des Datenschutzbeauftragten die Personen an, die zwischen Juli 2016 und Juni 2017 mit der Behörde in Kontakt waren. Insgesamt konnten mit der Befragung 376 Personen erreicht werden, wovon 181 den Fragebogen beantworteten, was eine sehr gute Antwortquote von rund 50 Prozent ergibt. Von den Teilnehmenden nahmen mehr als zwei Drittel als Mitarbeitende der kantonalen Verwaltung, der Gemeinden und anderer öffentlicher Organe eine Dienstleistung des Datenschutzbeauftragten in Anspruch. Rund 30 Prozent waren in der Privatwirtschaft beschäftigt oder hatten den Datenschutzbeauftragten als Privatpersonen kontaktiert.
Ein Drittel der Antwortenden nutzte die Dienste der telefonischen oder schriftlichen Rechtsberatung, gut 10 Prozent nahmen an Seminaren und Kursen teil. Ein Viertel hatte Kontakt mit den IT-Spezialisten des Datenschutzbeauftragten. Die Kundschaftsbefragung ist Bestandteil der Wirksamkeitsmessung entsprechend dem Zürcher Qualitätsmodells und der ISO 9001-Norm.

«In welcher Eigenschaft hatten Sie mit dem Datenschutzbeauftragten Kontakt?»



Durchschnittliche Beurteilung der Kundenzufriedenheit



Mittelwert 5,2

Entwicklungsschwerpunkte im KEF

Die Indikatoren im Konsolidierten Entwicklungs- und Finanzplan (KEF) zeigen, dass die Aufgaben beim Datenschutzbeauftragten stetig zunehmen, dies bei gleichbleibenden Ressourcen.

Die generelle Zunahme der Beratungen von Privatpersonen beim Datenschutzbeauftragten um rund zehn Prozent zeigt indirekt auch die Herausforderungen des Datenschutzes und der Informationssicherheit in der zunehmend digitalisierten Verwaltung.

Die Beratungen sind im vergangenen Jahr um über zehn Prozent angestiegen. Die ausgewiesenen 560 Beratungsfälle von Privatpersonen übersteigen die Zahl der mit den bestehenden personellen Ressourcen möglichen Beratungen von 500 Fällen pro Jahr. Die Beratungen konnten nur dank Zusatzleistungen erbracht werden, was aber für die Zukunft nicht mehr garantiert ist. In diesem Zusammenhang ist darauf hinzuweisen, dass dieser Indikator nur einen Teil der Leistungen des Datenschutzbeauftragten abbildet und eine Überschreitung von mehr als zehn Prozent kritisch ist.

Im vergangenen Jahr erarbeitete der Datenschutzbeauftragte auch mehr Vernehmlassungen, während die Anzahl der Informations- und Weiterbildungsdienstleistungen im geplanten Umfang lag.

Aufgrund fehlender Ressourcen und besonderer Umstände konnte die Anzahl der geplanten Kontrollen nicht erreicht werden. Nur ungefähr drei Viertel der geplanten Kontrollen konnten durchgeführt werden. Zu den besonderen Umständen gehörte, dass bei den Kontrollen im Vorjahr teilweise schwerwiegende Mängel gefunden worden waren. Dies erforderte zahlreiche zusätzliche Kontakte mit den verantwortlichen Organen. Einerseits ging es darum, die zu treffenden Massnahmen zu konkretisieren und einen Zeitplan für ihre Umsetzung zu definieren. Weiter stellte der Datenschutzbeauftragte fest, dass die in vergangenen Kontrollen ermittelten Mängel von vielen öffentlichen Organen nicht behoben worden waren. Häufig wurden keine Massnahmen getroffen. Wie der im KEF zusätzlich ausgewiesene Wirkungsindikator zeigt, wurden im vergangenen Jahr nur zirka 40 Prozent der im Rahmen von Datenschutzreviews erfolgten Hinweise umgesetzt. Diese unbefriedigenden Resultate führten den Datenschutzbeauftragten dazu, die Nachkontrollen bei Datenschutzreviews neu zu konzipieren (Seite 39). Diese Nachkontrollen bedeuten einen zusätzlichen Aufwand, da die öffentlichen Organe nicht in der vorgesehenen Frist reagierten. Für eine regelmässige und vertiefte Kontrolle der wichtigsten Datenbearbeitungen fehlen die notwendigen Ressourcen.

Leistungsindikatoren		KEF	2017
Beratungen	Der DSB berät öffentliche Organe und Privatpersonen in Fragen des Datenschutzes und der Informationssicherheit. Die Beratung erfolgt persönlich, telefonisch, per E-Mail oder Brief. Der Leistungsindikator im KEF misst die getätigten Beratungen von Privatpersonen.	500	560
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.	18	20
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.	20	21
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, Kontrollen auf Anlass sowie technische Kontrollen durch. Der Leistungsindikator im KEF gibt Auskunft über die realisierten Kontrollen.	40	31

Outsourcing und Cloud Computing

Cloud Computing im Trend

Die Auslagerung von Datenbearbeitungen in die Cloud bringt grundlegende Veränderungen mit sich. Daten lassen sich dadurch schnell, einfach, vielfältig, ortsunabhängig und zu niedrigen Kosten bearbeiten – der Attraktivität dieser Attribute können sich weder die Verwaltung noch die Privaten entziehen. Doch die Aspekte des Datenschutzes und der Informationssicherheit dürfen nicht in den Hintergrund treten.

Mangelnde Transparenz und Kontrollverlust

Im Gegensatz zu einer klassischen Auslagerung sind Cloud-Dienste standardisiert und die Nutzungs- und Vertragsbedingungen meistens vom Anbieter vorgegeben. Sie sind oft nicht datenschutzkonform. Das öffentliche Organ bleibt auch bei der Inanspruchnahme von Cloud-Diensten für die Datenbearbeitung verantwortlich, sieht sich aber mit neuen Risiken konfrontiert. So ist oft nicht bekannt, wo die Daten gespeichert werden und wer die Subauftragnehmer sind. Der Einfluss des Auftraggebers auf die Sicherheitsmassnahmen sinkt. Die neuen Risiken können unter den Begriffen unzureichende Transparenz und Kontrollverlust zusammengefasst werden.

Mit der Risikoanalyse anfangen

Bevor ein öffentliches Organ einen Cloud-Dienst einsetzt, muss es als Erstes klären, ob die Daten überhaupt ausgelagert werden dürfen. Wenn Geheimnispflichten dem entgegenstehen, kann allenfalls eine Verschlüsselung verhindern, dass Dritte Kenntnis von den Daten nehmen können. Weiter ist durch eine Risikoanalyse zu prüfen, ob die Sensitivität der Daten mit den Risiken einer Auslagerung in die Cloud zu vereinbaren ist. Kriterien sind beispielsweise das Datenschutzniveau des Landes, in dem die Daten gespeichert werden, oder die eingesetzte Technologie. Aufgrund des Resultats der Risikoanalyse müssen die Informationssicherheitsmassnahmen definiert werden. Erst jetzt kann die Auswahl eines Anbieters beginnen, mit dem ein datenschutzkonformer Vertrag ausgearbeitet wird.

Pflichten bleiben trotz Vertrag erhalten

Allein der Abschluss eines datenschutzkonformen Vertrags entbindet das öffentliche Organ nicht von weiteren Pflichten. Je nach Cloud-Dienst sind bei der konkreten Nutzung weitere organisatorische und technische Massnahmen zu berücksichtigen.

Schutz des Berufsgeheimnisses in der Cloud

Der Datenschutzbeauftragte wurde mehrfach angefragt, ob und wie Produkte zur Datenbearbeitung im Gesundheits-, Schul- oder Verwaltungsbereich eingesetzt werden können, die nur unter Nutzung einer Cloud funktionieren. Er hat abgeklärt, unter welchen Voraussetzungen das Berufsgeheimnis eine Auslagerung in die Cloud zulässt.

Cloud-Anbieter darf keine Kenntnis erlangen

Ein Gutachten von Dr. Wolfgang Wohlers, Professor für Strafrecht und Strafprozessrecht an der Universität Basel, befasst sich mit der Rechtslage einer Auslagerung unter Beachtung des Berufsgeheimnisses nach Art. 321 StGB. Wohlers kommt zum Schluss, dass Datenbearbeitungen, die dem Berufsgeheimnis unterliegen, nur in die Cloud ausgelagert werden können, wenn der Cloud-Anbieter von den Daten keine Kenntnis erlangen kann.

Verschlüsselung und vertragliche Absicherung

Der Bearbeitung im Auftrag dürfen grundsätzlich keine Geheimnispflichten entgegenstehen. Deshalb müssen die Daten verschlüsselt werden, um die Kenntnisnahme der Informationen durch Dritte zu verhindern. Gemäss Gutachten muss der Schlüssel beim Auftragnehmer verbleiben. Eine weitere Möglichkeit sieht der Datenschutzbeauftragte in der vertraglichen Absicherung. Der Auftragnehmer verpflichtet sich damit, den Schlüssel nur auf ausdrückliche Anfrage und nach ausdrücklicher Einwilligung des Auftraggebers einzusetzen und auf die Daten zuzugreifen. Ein Zugriff auf die Daten muss im Einzelfall auch möglich sein, wenn dies für die sachgerechte Erledigung des Auftrags notwendig und für den Geheimnisherrn vorhersehbar ist, etwa bei der Wartung medizinischer Geräte. Zudem kann immer ausgelagert werden, wenn die betroffene Person einwilligt. Das öffentliche Organ muss in jedem Fall alle zum Schutz der Daten notwendigen Sicherheitsmassnahmen umsetzen.

Dropbox & Co. in den Schulen

Cloud-Dienste sind aus dem Schulalltag nicht mehr wegzudenken. Der Datenschutzbeauftragte beschäftigt sich in der Beratungspraxis ständig mit Produkten wie Google Drive, Office 365, Apple School Manager, Lehrer Office und Dropbox.

Schulen bleiben für ihre Daten verantwortlich

Bei Cloud-Diensten ist auch im Schulbereich die sorgfältige Abklärung der datenschutzrechtlichen Aspekte zwingend. Nicht alles, was möglich ist, ist erlaubt. Die Nutzung von Cloud-Diensten ist eine Auslagerung der Datenbearbeitung. Die Schule bleibt auch in diesem Fall für ihre Daten verantwortlich.

Fragen zum Schutz der Privatsphäre und zur Sicherheit der Daten müssen vor dem Einsatz solcher Produkte geklärt werden. Die Schulverantwortlichen müssen sich überlegen, wie ein Produkt zu welchen Zwecken und mit welchen Daten genutzt werden soll. Sie müssen die Verantwortlichkeiten bestimmen und Zugriffe, E-Mail-Adressen, Authentifizierungsmechanismen und vieles mehr festlegen. Die Daten müssen klassifiziert und die Lehrpersonen sowie Schülerinnen und Schüler über eine korrekte Nutzung instruiert werden. Bei jüngeren Schülerinnen und Schülern müssen die Schulen die Eltern informieren, wenn im Internet personenbezogene Rückschlüsse möglich sind, weil beispielsweise die E-Mail-Adressen den vollständigen Namen des Kindes mit der Schule verbinden oder wenn sie auch zu Hause den Cloud-Dienst benutzen sollen.

Unterstützung bei den Verträgen

Schulen verfügen oft nicht über Expertenwissen zu den rechtlichen Aspekten einer Vertragsschliessung, weshalb sie sich an den Datenschutzbeauftragten wenden können. Für die Nutzung von Office 365 konnte mit dem Hersteller Microsoft eine datenschutzkonforme Lösung vereinbart werden. Dafür hat Educa.ch für die Volksschulen und Switch für die Hochschulen einen Rahmenvertrag mit dem Hersteller abgeschlossen. Die Schulen müssen die Beitrittserklärung zu diesem Vertragswerk ausfüllen und die erwähnten Massnahmen zum Schutz der Daten definieren und umsetzen.

«Die Risiken des Cloud Computing können unter den Begriffen unzureichende Transparenz und Kontrollverlust zusammengefasst werden.»

Cloud Computing in der Verwaltung

Der Datenschutzbeauftragte prüft vermehrt Verträge von Behörden, Spitälern und anderen öffentlichen Organen mit Cloud-Anbietern. Die Anfragen reichen von der Speicherung und Bearbeitung von Daten in einem Traumaregister über die Inanspruchnahme von Amazon Web Services und den Einsatz von E-Recruiting Tools, Austauschplattformen oder einer Newsletter-Software bis hin zur kompletten Auslagerung der IT-Infrastruktur.

In allen Fällen sind die Anforderungen des IDG umzusetzen. Das öffentliche Organ muss die Dienste sorgfältig auf die datenschutzrechtlichen Anforderungen überprüfen. Der Leitfaden Bearbeiten im Auftrag des Datenschutzbeauftragten beinhaltet Checklisten und Übersichten für das Vorgehen, die Vertragsbestimmungen und die zu implementierenden Informationssicherheitsmassnahmen.

Sicherheitsmassnahmen definieren

Beim Cloud Computing müssen im Rahmen einer Risikoanalyse die Informationssicherheitsmassnahmen definiert werden, die zum Schutz der Daten notwendig sind. Unterliegen die Daten dem Berufsgeheimnis, müssen sie immer verschlüsselt werden und das Schlüsselmanagement muss beim öffentlichen Organ liegen. Ist dies nicht möglich, sind zusätzliche vertragliche Absicherungen notwendig. Auf jeden Fall sollte das Land, in das die Datenbearbeitungen ausgelagert werden, über ein angemessenes Datenschutzniveau verfügen.

Transparenz der Auftragnehmer

Umfassende Transparenz des Auftragnehmers über die Sicherheitsmassnahmen, die Kontrollmöglichkeiten, die Subauftragnehmer und die Orte der Datenbearbeitung helfen, eine datenschutzkonforme und sichere Lösung zu finden.

Bevölkerungsbefragung mit Online-Tool

Eine Gemeinde führte unter anderem über ein Online-Tool auf ihrer Website eine Bevölkerungsbefragung durch. Eine Privatperson meldete dem Datenschutzbeauftragten, dass bei der Online-Befragung die IP-Adressen gespeichert würden und somit die Anonymität der Umfrageteilnehmenden nicht gewährleistet sei.

Der Datenschutzbeauftragte wandte sich zur Abklärung des Sachverhalts an die Gemeinde. Es zeigte sich, dass sie einen Dritten mit der Bevölkerungsbefragung beauftragt hatte, der wiederum das Online-Tool eines US-amerikanischen Anbieters einsetzte.

Antworten und Adressen nicht getrennt

Da die Umfrage mit der freiwilligen Teilnahme an einer Verlosung verbunden war, umfassten die gespeicherten Daten unter anderem die IP-Adresse, die Umfrageantworten sowie die Adresse für die Wettbewerbsteilnahme. Die Daten wurden zusammen in einem Datensatz abgespeichert. Die Speicherung der IP-Adresse und der Einsatz eines sogenannten IP-Blockers sollten die Mehrfachteilnahme an der Umfrage verhindern.

Der Auftragnehmer der Gemeinde exportierte die Datensätze aus dem Online-Tool und löschte die IP-Adressen. Die Adressdaten für die Wettbewerbsteilnahme trennte er von den Umfrageantworten und speicherte sie randomisiert ab. Die restlichen Daten speicherte er gemeinsam.

Ungenügende Vertragsbedingungen des Online-Anbieters

Der Datenschutzbeauftragte prüfte die Durchführung der Online-Umfrage sowie das Auslagerungsverhältnis zwischen der Gemeinde beziehungsweise dem von ihr beauftragten Dritten und dem Online-Tool-Anbieter. Er kam zum Schluss, dass die Datenerhebung personenbezogen durchgeführt worden war. Die Anonymität der Umfrageteilnehmenden war nicht gewährleistet, weil die Daten in jeweils einem Datensatz gespeichert wurden. Zudem beurteilte er die Speicherung der IP-Adresse als unverhältnismässig. Der Einsatz des IP-Blockers war nicht geeignet, die Mehrfachteilnahme zu verhindern, da die Umfrage auch in Papierform und durch Befragen von Passantinnen und Passanten erfolgt war. Weiter waren die Vertragsbedingungen des Online-Tool-Anbieters in verschiedener Hinsicht ungenügend und somit die Auslagerung der Personendaten in die USA nicht datenschutzkonform. Daraus folgerte der Datenschutzbeauftragte, dass die Gemeinde ihre Verantwortung, die sie gegenüber den Umfrageteilnehmenden am Schutz ihrer Personendaten trägt, ungenügend wahrgenommen hatte.

§ 8 IDG
§§ 6 IDG i.V.m. 21 IDV

Datennutzung

Datennutzung in der digitalen Verwaltung

Amtsstellen, Gemeinden, Schulen oder Gesundheitsinstitutionen ermöglichen der Bevölkerung, Transaktionen mit dem Gemeinwesen oder staatlichen Einrichtungen zunehmend digital abzuwickeln. Einwohnerinnen und Einwohner können heute bereits digital umziehen, Parkkarten beziehen, die Steuererklärung einreichen, eine Firma im Handelsregister anmelden oder eine Arbeitsbewilligung beantragen. Künftig sollen beispielsweise auch das Einbürgerungs- oder das Baubewilligungsverfahren elektronisch abgewickelt werden.

Vor- und Nachteile der Mehrfachnutzung von Daten

Daten zentral zu speichern und mehrfach zu nutzen, bringt viele Vorteile. Dies geschieht beispielsweise bei einem Bürgerkonto, über das eine Person alle Angelegenheiten mit dem Staat erledigen kann. Der Mensch wird dadurch aber gegenüber der Verwaltung immer gläserner, während die Datenflüsse im Hintergrund zunehmen und intransparenter werden.

Das Datenschutzrecht bestimmt, dass ein öffentliches Organ die Daten bearbeiten darf, die es zur Erfüllung seiner Aufgaben benötigt (§ 8 Abs. 1 IDG). Diese Aufgaben sowie jede Bearbeitung von besonderen Personendaten an sich müssen in einem Gesetz geregelt sein (§ 8 Abs. 2 IDG). Sollen Daten regelmässig an ein anderes öffentliches Organ weitergegeben werden, muss auch dieser Datenfluss gesetzlich geregelt sein (§§ 16 und 17 Abs. 1 IDG). Zudem ergibt sich aus dem Verhältnismässigkeitsprinzip (§ 8 Abs. 1 IDG), dass digitale Datenflüsse (File Transfer, Pull- oder Push-Dienste, Abrufverfahren usw.) nur die Daten beinhalten dürfen, die für die Aufgabenerfüllung des Datenempfängers geeignet und erforderlich sind.

Legalitätsprinzip bleibt massgebend

In der Praxis fehlen diese Rechtsgrundlagen häufig. Es genügt nicht, dass die mehrfache Datennutzung praktisch, effizient oder wirtschaftlich ist. Das Legalitätsprinzip ist in der öffentlichen Verwaltung wegweisend, was sich nicht nur aus dem IDG ergibt, sondern auch aus der Verfassung und den verwaltungsrechtlichen Prinzipien.

Frühzeitige Prüfung der Rechtsgrundlagen wichtig

Der Datenschutzbeauftragte empfiehlt, bei Digitalisierungsprojekten alle Datenbearbeitungen, Datennutzungen und Datenflüsse zu prüfen, ob sie vom geltenden Recht abgedeckt sind. Diese Prüfung findet am besten bereits in der Initialisierungs-, spätestens aber in der Konzeptphase statt, wie es auch in der Projektmanagementmethode Hermes beschrieben ist. Gleichzeitig kann geprüft werden, ob das Vorhaben vorabkontrollpflichtig ist (§ 10 IDG). Damit können auch rechtzeitig die notwendigen Rechtsgrundlagen geschaffen werden.

Weiterverwendung von Daten in der Forschung

Eine kantonale Amtsstelle gelangte im Zusammenhang mit einem Versorgungsforschungsprojekt an den Datenschutzbeauftragten. Sie hatte zwei Fachstellen Leistungsaufträge erteilt und ihnen damit eine öffentliche Aufgabe übertragen, in deren Rahmen sie Personendaten bearbeiten und in ihrer Datenbank abspeichern. Aus diesen Daten soll nun ein Register aufgebaut werden, das Aussagen zur Versorgungssituation ermöglicht, beispielsweise um Über- und Unterversorgungslagen im Kanton zu erkennen. Das neue Register soll fortlaufend die aktuellen Daten aus der Datenbank der Fachstellen beziehen. Die Datensätze des Registers sind deshalb über eine Schlüsselnummer der Datenbank zuordenbar. Das Register soll zudem die Daten für ein Versorgungsforschungsprojekt liefern.

Die Amtsstelle stellte dem Datenschutzbeauftragten die Frage, ob die betroffenen Personen hinsichtlich der zukünftig zu erhebenden Daten zwingend schriftlich in die Weiterverwendung der Daten für das Forschungsprojekt einwilligen müssten oder ob es wie in Bezug auf die Weiterverwendung der bereits erhobenen Daten ausreiche, sie über ihr Widerspruchsrecht aufzuklären.

Register an Fachstellen ausgelagert

Der Datenschutzbeauftragte zeigte auf, dass zwischen dem Aufbau und dem Betrieb des Registers und der Weiterverwendung der Daten für das Versorgungsforschungsprojekt zu unterscheiden ist. Der Betrieb des Registers dient der kantonalen Versorgungsplanung und damit einem Planungszweck, während die Weiterverwendung einen Forschungszweck verfolgt.

Für die Versorgungsplanung ist es ausreichend, anonymisierte Daten zu bearbeiten. Der Datenschutzbeauftragte wies zudem darauf hin, dass es sich um ein Outsourcing handelt, wenn das Register nicht von der kantonalen Amtsstelle, sondern von einer der beiden Fachstellen geführt wird.

Verwendung besonderer Personendaten nur mit ausdrücklicher Einwilligung

Die Weiterverwendung der Daten für das Versorgungsforschungsprojekt ist eine Zweckänderung, wofür eine Einwilligung der betroffenen Personen nötig ist. Da es sich bei den bearbeiteten Daten zudem um besondere Personendaten handelt, ist eine ausdrückliche Einwilligung erforderlich. Die Zustimmung muss also aktiv erteilt werden (Opt-in). Bleibt ein Widerspruch gegen die Weiterverwendung aus, kann dies nicht als Zustimmung gewertet werden (Opt-out). Die Einwilligung muss freiwillig und vorgängig erteilt werden. Der Datenschutzbeauftragte hielt fest, dass dies auch in Bezug auf die Weiterverwendung der bereits erhobenen Personendaten gilt.

§§ 9, 17 und 18 IDG

Adresslisten an Abstimmungskomitee

In einer Kirchgemeinde stand eine Urnenabstimmung bevor. Ein Mitglied eines Abstimmungskomitees wollte den Stimmberechtigten Abstimmungsinformationen zustellen und verlangte dafür bei der Einwohnerkontrolle die Adressen aller Kirchgemeindemitglieder.

Keine Listen nach Konfession

Einwohnerkontrollen können laut dem Gesetz über das Meldewesen und die Einwohnerregister (MERG) sogenannte Listenauskünfte erteilen. Sie können Adressdaten von Einwohnerinnen und Einwohnern nach bestimmten Kriterien geordnet bekannt geben, wenn diese für ideelle Zwecke verwendet und nicht weitergegeben werden. Die Konfession stellt jedoch kein solches Kriterium dar. Eine Listenauskunft darf deshalb nicht erteilt werden. Gemäss dem Verhältnismässigkeitsprinzip sind zudem Listenauskünfte ausgeschlossen, wenn die gewünschten Listen einen grossen Teil des Einwohnerstamms beinhalten.

Herausgabe des Stimmregisters nicht erlaubt

Im konkreten Fall wünschte das Abstimmungskomitee mit der Anfrage die Bekanntgabe des gesamten Stimmregisters der betreffenden Kirche. Dies widerspricht zusätzlich dem Gesetz über die politischen Rechte (GPR). Stimmberechtigten wird auf Verlangen zwar Auskunft über die Stimmberechtigung einer Person erteilt, jedoch nur im Einzelfall und in Bezug auf eine bestimmte Person (§ 9 Abs. 2 GPR, § 6 Verordnung über die politischen Rechte, VPR). Die Herausgabe des Stimmregisters oder eines Auszugs daraus ist nicht erlaubt.

§ 19 Abs. 1 MERG
§ 9 Abs. 2 GPR
§ 6 VPR
§ 16 Abs. 1 IDG

Fusionen von Sozialbehörden mehrerer Gemeinden

In einigen Gemeinden des Kantons Zürich sind Fusionen von Sozialbehörden zu interkommunalen Anstalten im Gang. Verschiedene Gemeinden wandten sich an den Datenschutzbeauftragten mit Fragen zum Austausch von Personendaten mit anderen öffentlichen Organen wie der Einwohnerkontrolle.

Interkommunale Anstalten arbeiten nicht im Auftragsverhältnis

Der Datenschutzbeauftragte hat zunächst darauf hingewiesen, dass es sich bei den neuen interkommunalen Anstalten um öffentliche Organe handelt, welche die ihnen übertragenen Aufgaben eigenständig ausüben und gestützt auf die Rechtsgrundlagen im Sozialhilfebereich selbstständig tätig werden. Es liegt kein Auftragsverhältnis vor. Der Datenaustausch richtet sich nach dem Verhältnismässigkeitsgrundsatz. Die interkommunalen Anstalten dürfen deshalb so weit Personendaten bearbeiten, als dies zur Erfüllung ihrer gesetzlich umschriebenen Aufgaben notwendig ist. Sie dürfen nur auf diejenigen Daten der Einwohnerkontrolle zugreifen, die ihre Klientinnen und Klienten betreffen, und auch nur auf diejenigen Personendaten oder Informationen, die sie zur Aufgabenerfüllung benötigen, also beispielsweise Namen oder Anzahl Mitbewohnerinnen oder Mitbewohner.

Zugriff auf die Daten aller Personen wäre unverhältnismässig

Ein Zugriff auf die Daten aller bei den Einwohnerkontrollen registrierten Personen wäre unverhältnismässig. Ein elektronisches Abrufverfahren kann deshalb nicht eingerichtet werden. Es kann aber eine Schnittstelle erstellt werden, über welche die Personendaten von bereits betreuten Klientinnen und Klienten ausgetauscht werden können. Bei neu hinzukommenden Klienten der Anstalt ist der zuständigen Einwohnerkontrolle eine Einzelanfrage zu stellen.

§ 8 IDG
§ 17 MERG

Zugriff Krebsregisterstelle auf Wohnsitzdatenbank

Die Gesundheitsdirektion und die Krebsregisterstelle des Kantons Zürich wandten sich mit Fragen zur Umsetzung des Datenbezugs der Krebsregisterstelle bei den Gemeinden an den Datenschutzbeauftragten. Das Krebsregistergesetz verpflichtet die Gemeinden, der Krebsregisterstelle jährlich die Personalien aller Personen bekannt zu geben, die im vorangegangenen Jahr in der Gemeinde wohnhaft waren. Sie können der Krebsregisterstelle dazu den direkten elektronischen Zugriff auf die Daten des Einwohnerregisters gewähren.

Zwischenlösung gesucht

Die Umsetzung dieser Regelung in allen Gemeinden hätte sowohl bei der Krebsregisterstelle als auch bei den Gemeinden erheblichen Aufwand verursacht. Die Kantonale Einwohnerplattform (KEP), die aus einer Kopie der kommunalen Einwohnerregister bestehen wird, ist erst im Aufbau. Nach ihrer Einführung wird die Krebsregisterstelle die erforderlichen Daten voraussichtlich daraus beziehen. Im Sinne einer Zwischenlösung stellte sich die Frage, ob der Krebsregisterstelle der Zugriff auf die Wohnsitzdatenbank der Gesundheitsdirektion eingeräumt werden kann.

Die Wohnsitzdatenbank dient der Gesundheitsdirektion, den Wohnsitz von Personen zu überprüfen, an deren Behandlungskosten sich der Kanton gemäss der Sozialversicherungsgesetzgebung des Bundes zu beteiligen hat oder die ein Gesuch um Befreiung vom Krankenversicherungsobligatorium gestellt haben. Sie enthält einen Teil der in den kommunalen Einwohnerregistern geführten Daten und umfasst die Personendaten, welche die Krebsregisterstelle benötigt.

Keine erhöhten Risiken für betroffene Personen

Der Datenschutzbeauftragte prüfte das geplante Vorgehen und kam zum Schluss, dass der Datenbezug aus der Wohnsitzdatenbank der Gesundheitsdirektion aus datenschutzrechtlicher Sicht keine erhöhten Risiken für die betroffenen Personen beinhaltet. Die Gesundheitsdirektion erarbeitete daraufhin eine Änderung der Wohnsitzprüfungsverordnung. Der Datenschutzbeauftragte begrüsste die Änderung. Damit wurden die notwendigen Rechtsgrundlagen für den Datenbezug der Krebsregisterstelle bei der Wohnsitzdatenbank der Gesundheitsdirektion geschaffen. Der Datenschutzbeauftragte nahm zu einzelnen Aspekten Stellung, die von der Gesundheitsdirektion berücksichtigt wurden.

§§ 17 i.V.m. 23 IDG
§ 5 Krebsregistergesetz
§§ 1 und 5 Wohnsitzprüfungsverordnung

Verordnung über das Meldewesen und die Einwohnerregister

Die Verordnung über das Meldewesen und die Einwohnerregister (MERV) regelt insbesondere das Verfahren zum Bezug und zur Bekanntgabe von Daten aus der Kantonalen Einwohnerdatenplattform (KEP). Das mit der Ausarbeitung der Verordnung beauftragte Gemeindeamt lud den Datenschutzbeauftragten zur Mitwirkung ein. Er wurde regelmässig über Entwürfe der MERV informiert und konnte das Gemeindeamt aus datenschutzrechtlicher Sicht beraten. Schliesslich nahm er am Vernehmlassungsverfahren teil. Der Datenschutzbeauftragte begrüsste diese enge und gute Zusammenarbeit.

Einwohnerregister insgesamt sensibel

Der Datenschutzbeauftragte wies darauf hin, dass die KEP als Ganzes und unabhängig von den bearbeiteten Personendaten sensibel ist, dies aufgrund der Anzahl der betroffenen Personen, der Anzahl der zugriffsberechtigten Personen sowie der Tatsache, dass die Daten im Abrufverfahren zur Verfügung stehen.

Protokollierung als Massnahme gegen Missbrauch

Der Datenschutzbeauftragte hielt fest, dass aus Transparenzgründen die Datenbezüger und die von ihnen bezogenen Personendaten in einem Anhang aufgeführt werden müssen. Weiter beriet er das Gemeindeamt bei Fragen zur Protokollierung und ihrer regelmässigen Auswertung, zur Zugriffsberechtigung sowie zu möglichen Massnahmen gegen Missbräuche.

Im Rahmen der Vernehmlassung begrüsste der Datenschutzbeauftragte die abschliessende Aufzählung der zusätzlich im Einwohnerregister erfassten Personendaten sowie die Auflistung der möglichen Datenbezüger und der abrufbaren Personendaten in einem Anhang. Er wies zudem darauf hin, dass mit der Protokollierung auch zu dokumentieren ist, auf welche Personendaten zugegriffen wurde, damit mögliche Missbräuche nachgewiesen werden können.

§ 24 Abs. 4 IDV
§ 3 [Abs. 4] lit. a IDG
§ 12 IDG
§ 8 IDG
§ 7 IDG

Datenaustausch zwischen Statthalterämtern und der Polizei

Die Änderung des Gesetzes über die Gerichts- und Behördenorganisation (GOG) regelt den gegenseitigen direkten elektronischen Zugriff auf Daten durch die Statthalterämter und die Polizei bei der Verfolgung und Beurteilung von Übertretungen.

Notwendige gesetzliche Grundlage geschaffen

Die Bestimmung schafft die für einen Austausch von besonderen Personendaten notwendige gesetzliche Grundlage, wie sie bereits besteht für den Datenaustausch zwischen Staatsanwaltschaften und Polizei. Da der Zugriff auf die für die Aufgabenerfüllung notwendigen Daten beschränkt ist, begrüsste der Datenschutzbeauftragte die Regelung.

Anfragen der Bezirksgerichte an die Jugendhilfestellen

Die Bezirksgerichte stellen den Jugendhilfestellen in hängigen Eheverfahren standardmässig Formulare zu, mit denen um Mitteilung über Informationen gebeten wird, die im Hinblick auf die Kinderzuteilung oder die Gestaltung des Besuchsrechts wichtig sind. Das Amt für Jugend und Berufsberatung fragte den Datenschutzbeauftragten, wie diese Anfragen datenschutzrechtlich zu behandeln sind.

Entbindung von Geheimnispflichten nötig

Der Datenschutzbeauftragte stellte fest, dass es sich um eine Datenbekanntgabe handelt, für die eine hinreichend bestimmte Grundlage in einem formellen Gesetz nötig ist. Diese Voraussetzung erfüllt Art. 190 Zivilprozessordnung (ZPO). Vor einer Auskunftserteilung muss der betreffende Mitarbeitende jedoch von der vorgesetzten Behörde vom Amtsgeheimnis und allenfalls vom Berufsgeheimnis entbunden werden. Dies ergibt sich zwar nicht aus dem Wortlaut von Art. 190 ZPO, jedoch aus Lehre und Rechtsprechung. Eine Entbindung verlangt auch § 143 Abs. 1 Vollzugsverordnung zum Personalgesetz (VVO), die für kantonale Angestellte und häufig auch für Gemeindeangestellte gilt.

Ausnahme, wenn kein Geheimnisinteresse besteht

Im konkreten Fall stellte sich die Frage, ob bereits die Information unter das Amts- oder Berufsgeheimnis fällt, dass die Jugendhilfestelle über keine Hinweise verfüge, die im Hinblick auf die Kinderzuteilung oder die Gestaltung des Besuchsrechts wichtig sind.

Ein Geheimnis ist eine Tatsache, die einem begrenzten Personenkreis bekannt ist, welche die Person geheim halten will und an deren Geheimhaltung sie ein berechtigtes Interesse hat. Die Angestellten sind zur Geheimhaltung über dienstliche Angelegenheiten verpflichtet, wenn ein überwiegendes öffentliches oder privates Interesse besteht oder wenn eine besondere Vorschrift dies vorsieht. Im vorliegenden Fall besteht kein berechtigtes öffentliches oder privates Interesse an der Geheimhaltung. Mit der Information, über keine Hinweise zu verfügen, legt die Jugendhilfestelle nicht offen, ob ihr die Eltern oder das Kind bekannt sind. Die Mitteilung ist datenschutzrechtlich zulässig und da kein Geheimhaltungsinteresse besteht, bedarf diese Auskunft keiner Entbindung vom Amts- oder Berufsgeheimnis.

Art. 190 ZPO
§ 17 i.V.m. § 23 IDG
Art. 320 und 321 Strafgesetzbuch (StGB)
§ 43 VVO

Informationssicherheit

Informationssicherheit ist ein kontinuierlicher Prozess

Die heutigen Technologien bieten die Möglichkeit, Dienstleistungen rund um die Uhr anzubieten und zu nutzen. Wer von den Chancen der Digitalisierung nachhaltig profitieren will, muss die Risiken kontinuierlich bewerten und Sicherheitsvorkehrungen treffen.

Die Grundprinzipien des Datenschutzes und der Informationssicherheit, nämlich Vertraulichkeit, Verfügbarkeit und Integrität müssen jederzeit gewährleistet sein. Dafür müssen alle Funktions- und Managementstufen die auf die Sicherheit ausgerichteten Vorgaben und Prozesse erkennen und umsetzen.

Informationssicherheitskonzepte

Die Vorgaben und Richtlinien für eine integrale Informationssicherheit müssen auf der strategischen, taktischen und operativen Ebene erstellt und umgesetzt werden. Die Dokumente reichen von der Leitlinie zur Informationssicherheit über das Informationskonzept bis zu den Checklisten und Verträgen. Der Datenschutzbeauftragte stellt auf seiner Website eine Übersicht der Dokumente sowie weitere Vorlagen zur Verfügung.

Der Schutz der Privatsphäre als Standard in der Planung

Mit Privacy by Design werden der Datenschutz und der Schutz der Privatsphäre als Teil des Konzepts bereits bei der Planung konsequent beachtet, während bei Privacy by Default darauf geachtet wird, dass standardmässig die höchste Stufe des Schutzes der Privatsphäre gewählt wird. Diese beiden Ansätze gewährleisten den Datenschutz und die Informationssicherheit während der Umsetzung eines Vorhabens oder Projekts.

Sicherheit von Websites

Ein unsachgemässer Aufbau oder Betrieb einer Website kann zu Verletzungen von Datenschutz- oder Geheimhaltungsvorschriften führen. Daher müssen bestimmte Sicherheitsmassnahmen umgesetzt und periodisch kontrolliert werden.

Awareness und Sensibilisierung

Auch wenn die Sicherheitsmassnahmen implementiert, regelmässig kontrolliert und in einem geregelten Risikomanagementprozess überprüft werden, so bearbeiten letztendlich die Mitarbeitenden die Informationen. Sie sind oft das Ziel von Spam-, Phishing- und Social-Engineering-Attacken. Die Sensibilisierung der Mitarbeitenden reduziert diese Risiken.

Informationssicherheit ist ein kontinuierlicher Prozess, an dem sämtliche Funktionen und Mitarbeitenden beteiligt sein müssen. Nur so kann die Digitalisierung erfolgreich, sicher und zukunftsgerichtet umgesetzt werden.

Beispielhafte Informationssicherheit

Im Rahmen einer Beratung beurteilte der Datenschutzbeauftragte die Dokumente zur Informationssicherheit sowie die Notfallbetriebsplanung einer Hochschule. Der Datenschutzbeauftragte kam zum Schluss, dass die geprüften Dokumente eine gute Ausganglage für eine umfassende Informationssicherheit bilden.

In der Leitlinie für die Informationssicherheitsziele definierte die Hochschule die angestrebte Sicherheitskultur, Klassifizierungskriterien sowie die Sicherheitsorganisation. Die wichtigsten Verantwortlichkeiten und Aufgaben für die wichtigsten Rollen wurden wie folgt definiert:

Hochschulleitung

- Gesamte Verantwortung für Informationssicherheit und Datenschutz
- Genehmigt die Informationssicherheitsstrategie und die Ressourcen
- Abnahme der Risiken und des jährlichen Sicherheitsberichts

Informationssicherheitsausschuss

- Zuständig für die normative Informationssicherheit
- Entscheidet über Sicherheitsmassnahmen
- Bereitet den jährlichen Sicherheitsbericht für die Hochschulleitung vor
- Mitglieder sind die Verwaltungsdirektorin oder der Verwaltungsdirektor, die Datenschutzverantwortlichen und die Informationssicherheits-Verantwortlichen

Informationssicherheits-Verantwortliche

- Verantwortlich für die operative Informationssicherheit
- Zentrale Ansprechstelle für sämtliche Fragen der Informationssicherheit
- Beraten und schulen die Mitarbeitenden in sämtlichen Fragen der Informationssicherheit
- Begleiten und kontrollieren die Projekte sowie den Betrieb bei der korrekten Umsetzung und bei der Einhaltung der Sicherheitsmassnahmen
- Bei Sicherheitsvorfällen zuständig für die Information und die Eskalation an den Informationssicherheitsausschuss

Anwendungs- und Systemverantwortliche

- Gewährleisten die Sicherheit der in ihrer Verantwortung liegenden Werte der Hochschule
- Stellen die nötigen Sicherheitsmassnahmen auf der Basis anerkannter Standards wie ISO 27002 oder der Bausteine des BSI sicher
- Kontrollieren die Einhaltung und Umsetzung der Konzepte Privacy by Default und Privacy by Design

Termineinladungen mit E-Mail oder SMS

Ein Spital plante, den Patientinnen und Patienten die Termineinladung per E-Mail und die Erinnerung per SMS zu verschicken, und bat den Datenschutzbeauftragten, das Vorhaben aus datenschutzrechtlicher Sicht zu beurteilen.

Der vorgesehene Inhalt der elektronischen Mitteilungen umfasste die Datumsangaben des Termins, die medizinischen Vorbereitungen wie «nüchtern» oder «mit voller Blase», Informationen zur Behandlung oder zur Untersuchung wie die Aufklärung über die Gefahren einer Darmspiegelung sowie einen Fragebogen und einen personifizierten Link zur Einverständniserklärung für die Behandlung.

Der Datenschutzbeauftragte stellte fest, bereits die Tatsache, dass sich eine Person bei einem Spital in medizinischer Behandlung befindet, falle unter die ärztliche Schweigepflicht. Für eine Termineinladung und -erinnerung per E-Mail oder SMS muss die Patientin oder der Patient deshalb in die Aufhebung der Schweigepflicht einwilligen (sogenanntes Opt-in). Die Wahlmöglichkeit zwischen der herkömmlichen Einladung und Erinnerung per Post und der digitalen Kontaktaufnahme muss weiterhin bestehen.

Entscheidet sich eine Patientin oder ein Patient für die digitale Kommunikation mit dem Spital, so wäre ein möglicher datenschutzkonformer Ansatz, Statusmeldungen per SMS oder E-Mail zu verschicken und die eigentlichen Informationen über eine geschützte Website anzubieten. Vor dem Zugang zur Information müsste sich die Patientin oder der Patient eindeutig identifizieren. Beim Aufbau einer solchen Lösung sind die Sicherheitsmassnahmen durch eine Risikoanalyse, die anerkannten Standards und die Best Practices zu definieren, um Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit und Authentizität zu gewährleisten. Informationen, die Rückschlüsse auf die Gesundheit einer Person zulassen, müssen grundsätzlich mit starker Verschlüsselung und Zwei-Faktor-Authentifizierung geschützt werden.

Webchecks decken Schwachstellen auf

Im Jahr 2017 hat der Datenschutzbeauftragte zahlreiche Sicherheitsüberprüfungen von Websites öffentlicher Organe, sogenannte Webchecks, durchgeführt.

Dabei werden die Websites mit Programmen gezielt auf bekannte Sicherheitslücken und Schwachstellen durchleuchtet. Komplexe Schwachstellen überprüft der Datenschutzbeauftragte zusätzlich manuell.

Die Liste der Schwachstellen, die durch die Webchecks gefunden wurden, deckt sich weitgehend mit der Schwachstellen-Top-10 des Open Web Application Security Project (OWASP).

So speicherten drei der geprüften Websites die Passwörter im Klartext – eine Schwachstelle mit grossem Missbrauchspotenzial. Moderne Anwendungen speichern Passwörter immer in verschlüsselter Form.

In zwei weiteren Fällen wurden Schwachstellen gefunden, die es Angreifern ermöglichen, eigene Befehle in die SQL-Datenbank einzuschleusen. Mit einer sogenannten SQL Injection können die gespeicherten Daten ausgespäht und verändert werden. Angreifer können selbst die Kontrolle über den Server übernehmen.

Der Datenschutzbeauftragte forderte die Website-Betreiber auf, diese gravierenden Sicherheitslücken umgehend zu schliessen.

Sensibilisierungs-veranstaltung für Mitarbeitende

Ein öffentliches Organ wollte seine Mitarbeitenden für Fragen der Informationssicherheit sensibilisieren und bat den Datenschutzbeauftragten um Unterstützung. Er bot eine einstündige Schulung vor Ort an, während der die Teilnehmerinnen und Teilnehmer die Risiken, Gefahren und möglichen Massnahmen interaktiv erarbeiteten.

Nachdem die Bedeutung des Schutzes der Persönlichkeit und der Privatsphäre erklärt worden war, lernten die Teilnehmenden konkrete Strategien und Hilfsmittel kennen, welche die Informationssicherheit im Alltag verbessern.

Vorgestellt wurden:

- Möglichkeiten der sicheren Datenübermittlung mit IncaMail oder WebTransfer ZH
- Hilfsmittel für den Umgang mit Passwörtern wie der Passwortcheck oder verschiedene Passwortmanager
- Sicherheitsvorkehrungen für Smartphones und mobile Geräte

Check & Balance

Wirkung der Datenschutzreviews verstärken

Der Datenschutzbeauftragte überprüft mit Kontrollen, ob die öffentlichen Organe die Anforderungen des Datenschutzes in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht einhalten. Das Spektrum der zu kontrollierenden Organe umfasst alle Ämter der kantonalen Verwaltung und der über 160 Gemeinden, die Spitäler und Schulen sowie weitere Institutionen wie Alters- und Pflegeheime, Staatsanwaltschaften und Notariate.

Mit den vorhandenen Ressourcen kann der Datenschutzbeauftragte die ungefähr tausend Institutionen nicht regelmässig überprüfen. Er hat verschiedene Massnahmen ergriffen, um die Aufsichtspflicht trotzdem zu erfüllen und die Wirksamkeit der Kontrollen zu optimieren. Der Datenschutzreview wurde neu konzipiert, und es werden zunehmend Auftragnehmer kontrolliert, die für zahlreiche öffentliche Organe tätig sind.

Optimierter Datenschutzreview

Die Neukonzipierung der Datenschutzreviews verfolgt die folgenden Ziele:

- Erfassung aller zu prüfenden Institutionen und Objekte
- Einführung eines risikobasierten Ansatzes mit nachvollziehbarer Bewertung als Grundlage zur Jahresprüfplanung
- Einführung einer detaillierten Jahresprüfplanung
- Neugestaltung des Prüfprogramms für Datenschutzreviews in Anlehnung an die Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die Normen ISO 27001/ISO 27002
- Detaillierte Darstellung der Massnahmen und der damit adressierten Risiken in den Berichten zur Verbesserung der Verständlichkeit bei den geprüften Organen sowie des Nachvollzugs
- Einführung von abgestuften Umsetzungsterminen je nach Risiko und Aufwand
- Einführung einer Stellungnahme zur Umsetzung der Massnahmen durch die geprüften Organe, um diese in den Lösungsprozess einzubeziehen und eine grössere Akzeptanz zu erreichen

Die neue Prüfmethodik und die neue Berichtsform werden seit Anfang 2017 angewendet.

Kontrolle von Outsourcingnehmern

Gemeinden und andere öffentliche Organe lagern ihre IT-Leistungen zunehmend aus. Deshalb entwickelte der Datenschutzbeauftragte ein Konzept zur Prüfung der Auftragnehmer mit den folgenden drei Zielen:

- Prüfung der Informationssicherheit dort, wo die Leistungen erbracht werden, bei Outsourcings also beim Auftragnehmer und nicht primär bei den Gemeinden
- Verbesserung der Effizienz und der Nutzung des Synergieeffekts, indem durch die Prüfung von Auftragnehmern Rückschlüsse auf alle angeschlossenen öffentlichen Organe gezogen werden können, so dass diese nicht umfassend geprüft werden müssen
- Erweiterung der Wissensbasis des Datenschutzbeauftragten über die bei den Auftragnehmern eingesetzten Technologien und Prozesse sowie Schaffung von Vergleichsmöglichkeiten

Der Prüfumfang wurde wie folgt festgelegt:

- Informationssicherheitsstrategie sowie Einsatz von Informationssicherheits-Managementsystemen (ISMS)
- Informationssicherheitskonzept (Risikoanalyse, Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Verfügbarkeit der IT-Systeme (Notfallvorsorge, Back-up und Restore)
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten)
- Clients/Server (Grundkonfiguration und Verwaltung)
- Physische Schutzmassnahmen gegen Umwelteinflüsse sowie Zutrittsrechte
- Outsourcing (Verträge, Kontrollmittel, Betriebskonzept sowie -handbücher, insbesondere Back-up-Konzept, Incident-Management-Prozess, Sicherheitsmassnahmen, Verschlüsselung, Protokollierung und Auswertung bei besonderen Personendaten, Entsorgung von Datenträgern)
- Regelung des Passwortgebrauchs und technische Umsetzung
- Netzwerke (Übersicht Verbindungen, Provider, Anbindung, drahtlose Netzwerke)
- Rollen- und Berechtigungskonzept (Rolle des Datenverantwortlichen, Klassifizierung von Daten, administrative Prozesse für Zugriffe und Passwörter), Umsetzung, Aktualitätskontrolle
- Mobile Arbeitsplätze, Smartphones und mobile Datenträger (Bewilligung, Richtlinien, Schulung, Schutzmassnahmen wie Verschlüsselung, Passwort, Softwareupdates, Back-up)
- Weisungen für Benutzerinnen und Benutzer (PC/Client, Passwörter, E-Mail und Internet)
- Interne und externe Überprüfung der Informationssicherheit

Der Datenschutzbeauftragte erstellte eine Liste der Auftragnehmer, die IT-Dienstleistungen für öffentliche Organe erbringen, und priorisierte sie nach ihrer Verbreitung und ihrem Marktanteil. Darauf definierte er einen Fragenkatalog für Auftragnehmer und einen für die angeschlossenen öffentlichen Organe, mit dem die Resultate der Auftragnehmerprüfung verifiziert werden sollen. In der nächsten Phase überprüfte der Datenschutzbeauftragte einen öffentlich-rechtlichen und einen privatrechtlichen Outsourcingnehmer. Mit einer Kontrolle bei drei Gemeinden, die unterschiedliche Dienstleistungen vom privat-rechtlichen Outsourcingnehmer beziehen, wurden die Resultate verifiziert.

Die Umsetzung des Konzepts verlief erfolgreich, weshalb im Lauf der nächsten Jahre weitere Auftragnehmer geprüft werden.

Überprüfung eines öffentlich-rechtlichen Auftragnehmers

Ein öffentliches Organ, das sämtliche IT-Dienstleistungen von einer kantonalen Organisationseinheit bezieht, fragte den Datenschutzbeauftragten an, den Schutz der ausgelagerten Daten zu prüfen. Die kantonale Organisationseinheit erbringt Leistungen für 40 angeschlossene Institutionen und rund 1800 Arbeitsplätze in der kantonalen Verwaltung. Sie betreibt für verschiedene Amtsstellen eine Sicherheitsinfrastruktur. Die Risikoeinstufung der Organisationseinheit wurde anhand eines Bewertungsrasters als hoch eingestuft, da mehr als 1000 Systeme und mehr als 50 000 betroffene Personen festgestellt wurden.

Die Prüfung zeigte, dass die Organisationseinheit einen stabilen und gegen grössere Ausfälle abgesicherten Betrieb für ihre Kunden erbringt. Weiter ist ein Informationssicherheitsmanagement etabliert und wichtige Dokumente wie eine Strategie, ein IT-Sicherheitskonzept sowie ein Qualitätsmanagement sind vorhanden.

Mängel im organisatorisch-technischen Bereich bestehen etwa im Bereich von Weisungen, Vorgaben und bei der Umsetzung in Bezug auf verschiedene IT-sicherheitsrelevante Themen. Zudem sind besondere Personendaten auf Servern von Softwarelieferanten gespeichert. Der Datenschutzbeauftragte stellte weiter Schwachpunkte beim Netzwerk und Verbesserungspotenzial bei den Prozessen im Bereich der Zugriffsberechtigungen fest. Er erhielt bislang keine Rückmeldung bezüglich der Umsetzung der Massnahmen.

Datenschutzreview eines privaten Auftragnehmers

Der Outsourcingnehmer erbringt verschiedene IT-Dienstleistungen für private Unternehmen wie auch öffentliche Organe. Neben Softwarelösungen bietet er auch Systemlösungen wie eine Schweizer Cloud an. Rund 50 Zürcher Gemeinden und Städte beziehen Dienstleistungen dieses Outsourcingnehmers. Er ist nach der Norm für Informationssicherheits-Managementsysteme ISO 27001 zertifiziert. Das Risiko des Outsourcingnehmers wurde anhand eines Bewertungsrasters als hoch eingestuft.

Der Datenschutzbeauftragte prüfte beim Outsourcingnehmer neben den organisatorischen und technischen auch juristische Fragen wie die Gewährleistung des Datenschutzes und der Informationssicherheit in Verträgen mit Auftraggebern sowie die Aufbewahrungsdauer, Archivierung und Löschung von Personendaten.

Die Kontrolle zeigte, dass das Unternehmen über ein etabliertes Informationssicherheits-Managementsystem (ISMS) verfügt, das in der Organisation gut verankert ist. In den zentralen rechtlichen, organisatorischen und technischen Prüfbereichen setzt das Unternehmen die Anforderungen des Datenschutzes und der Informationssicherheit umfassend um.

In einzelnen Prüfbereichen sind Optimierungen möglich, beispielsweise kann die Rolle eines internen Datenschutzverantwortlichen geschaffen, sollten die Daten bei der Übermittlung und Speicherung verschlüsselt, ein umfassenden Protokollierungskonzepts erstellt und schliesslich die Verträge mit den Kunden der öffentlichen Verwaltung an die Vorgaben des Kantons Zürich angepasst werden.

Wie erwartet verringerte die Prüfung des Auftragnehmers den Prüfungsaufwand bei den angeschlossenen Gemeinden. Durch die Prüfung des Outsourcingnehmers konnten Rückschlüsse auf insgesamt 19 Gemeinden gezogen werden, die Kunden sind.

Nachkontrolle der Massnahmen-umsetzung

Im Jahr 2017 prüfte der Datenschutzbeauftragte die Umsetzung aller seit 2014 bei Kontrollen empfohlenen Massnahmen. Dafür wurden die geprüften Organe angeschrieben und um Rückmeldung über den Stand der Umsetzung gebeten.

Oft verliefen die Rückmeldungen schleppend oder erfolgten gar nicht. Zudem zeigten die Nachkontrollen, dass die Massnahmen ungenügend umgesetzt worden waren. Teilweise waren gar keine Verbesserungen festzustellen.

Der Datenschutzbeauftragte beschloss, die Nachkontrollen zu intensivieren, um die Wirkung und Nachhaltigkeit der Datenschutzreviews sicherzustellen. Er entwickelt deshalb 2017 ein Konzept zur ständigen Nachkontrolle aller Massnahmen. Damit wird gewährleistet, dass die angetroffenen Risiken und Sicherheitslücken zeitnah behoben werden und die Kontrollen die gewünschte Verbesserung der Informationssicherheit bewirken.

Weitere Themen

Datenerhebung im Sozialbereich

Der Datenschutzbeauftragte hat sich mit unterschiedlichen Fragen zur Art und Weise befasst, wie Personendaten im Sozialbereich erhoben werden.

Einforderung detaillierter Bankauszüge

Mehrere Personen wandten sich mit Fragen zu Datenerhebungen durch kommunale Sozialämter an den Datenschutzbeauftragten. Die betroffenen Personen wurden von den Sozialhilfebehörden aufgefordert, vollständige, detaillierte Bankauszüge einzureichen.

Der Datenschutzbeauftragte wandte sich an das Sozialamt des Kantons Zürich und klärte die Praxis und die Rechtslage ab. Unter Hinweis auf die Rechtsprechung des Verwaltungsgerichts des Kantons Zürich erläuterte das Sozialamt des Kantons Zürich nachvollziehbar, dass die Sozialbehörden befugt sind, detaillierte Bankauszüge zu verlangen.

Einsatz von Sozialdetektivinnen und Sozialdetektiven

Der Europäische Gerichtshof für Menschenrechte (EGMR) ist im Oktober 2016 in seinem Urteil Vukota-Bojic gegen Schweiz Nr. 61838/10 zum Schluss gekommen, dass die schweizerischen Regelungen für den Einsatz von Privatdetektivinnen und Privatdetektiven durch Unfallversicherungen dem Erfordernis der Vorhersehbarkeit nicht genügen. Entsprechend stellte er eine Verletzung des Grundrechts auf Privatsphäre fest.

Der Datenschutzbeauftragte analysierte das Urteil und beurteilte die Rechtslage für den Einsatz von Privatdetektivinnen und Privatdetektiven im Bereich der Sozialhilfe im Kanton Zürich.

Er kam zum Schluss, dass auch die Bestimmungen im Sozialhilfegesetz des Kantons Zürich (SHG) keine ausreichende Rechtsgrundlage für den Einsatz von Privatdetektivinnen und Privatdetektiven darstellt, und entsprechend gesetzgeberischer Handlungsbedarf besteht. Sein Ergebnis hat der Datenschutzbeauftragte im Webartikel «EGMR-Urteil und der Einsatz von Sozialdetektivinnen und Sozialdetektiven» publiziert.

Der Datenschutzbeauftragte hat diese Erkenntnisse auch der Sicherheitsdirektion mitgeteilt. Die Sicherheitsdirektion teilte seine Auffassung jedoch nicht und sah keinen Handlungsbedarf.

Stellungnahme zur Änderung des ATSG

In der Folge des Urteils des EGMR wurde auf Bundesebene eine Änderung des Bundesgesetzes über den Allgemeinen Teil der Sozialversicherungsrechts (ATSG) vorgeschlagen. Im Vernehmlassungsverfahren hat der Datenschutzbeauftragte die Regelung begrüsst, weil sie in einem Gesetz erlassen werden soll, was aufgrund des schweren Grundrechtseingriffs erforderlich ist. Zudem wird durch die Gesetzesänderung der Einsatz von Privatdetektivinnen und Privatdetektiven auch für andere Versicherungsbereiche geregelt, die dem ATSG unterstehen.

Stellungnahme zur Totalrevision des Sozialhilfegesetzes

Auch im Mitberichtsverfahren zur Totalrevision des Sozialhilfegesetzes des Kantons Zürich nahm der Datenschutzbeauftragte zur Observation Stellung. Er hielt fest, dass aus grundrechtlicher Sicht der Einsatz von Geräten zur Ortung der betroffenen Person bei einem Verwaltungsverfahren weder zumutbar noch verhältnismässig ist und den Kerngehalt des Grundrechts auf Privatsphäre tangiert. Der Datenschutzbeauftragte merkte zudem an, dass die bestehende Bestimmung im SHG weder als Rechtsgrundlage für angekündigte noch für unangemeldete Hausbesuche ausreicht, und schlug vor, Hausbesuche in einem eigenen Paragraphen zu regeln. Schliesslich wies der Datenschutzbeauftragte auf Aspekte hin, die im Gesetzesentwurf noch nicht enthalten sind, wie die Informationsbearbeitung an sich. Darunter fallen die Aufbewahrung, der Zugriff, die Weitergabe, die Löschung sowie das Einsichtsrecht der betroffenen Person.

§ 8 IDG
§ 18 SHG

Anonymisierung gesundheitsbezogener Personendaten

Ein Forschungsinstitut legte dem Datenschutzbeauftragten ein Anonymisierungskonzept für die Durchführung einer Medikamentenstudie vor. Darin war vorgesehen, dass das Forschungsinstitut von einem Krankenversicherer eine grosse Anzahl Rechnungsdaten erhält. Diese geben Auskunft über die versicherte Person (Alter, Geschlecht, Wohnkanton, Franchise), ihren Medikamentenbezug sowie die ärztlichen Behandlungen (ambulant, stationär, Notfall, Code der Fallpauschale) während eines Zeitraums von zwei Jahren. Die Datensätze waren mit einer Studien-ID anonymisiert. Der Datenschutzbeauftragte prüfte das Konzept und riet bei zwei zentralen Aspekten zu Verbesserungen.

Im Anonymisierungskonzept leitet sich die Studien-ID aus der Versichertennummer ab. Die Anonymisierung erfolgt, indem zweimal eine Hash-Funktion angewendet wird, zunächst beim Versicherer und anschliessend beim Forschungsinstitut, worauf der Schlüssel vernichtet wird. Der Datenschutzbeauftragte erachtete dieses Vorgehen als gut, empfahl allerdings eine Anpassung der Hash-Funktion, um die Effektivität der Umwandlung zu erhöhen.

Zudem war für den Datenschutzbeauftragten entscheidend, ob einzelne Versicherte durch ihr individuelles Profil aus der Masse der Datensätze hervortreten und so bestimmbar sind. Am heikelsten erschien die Erhebung des Arzneimittels und des Codes der Fallpauschalen. Er empfahl, Daten über Versicherte, die ein seltenes Medikament verschrieben bekamen oder einer seltenen Fallgruppe zugeordnet wurden, vor der Übermittlung aus den Studiendaten zu löschen. Der Datenschutzbeauftragte schlug zudem vor, Altersgruppen zu bilden (z.B. Jahrgänge 1960–1965), statt das Geburtsjahr der versicherten Personen zu melden, was das Risiko verringert, dass die Person identifiziert werden kann.

Der Datenschutzbeauftragte stellte fest, dass die Anonymität der Daten gewährleistet sei, falls die empfohlenen Massnahmen umgesetzt werden und das Forschungsinstitut die Daten nicht mit weiteren Datenbeständen zusammenführt oder abgleicht.

§§ 3 und 8 IDG
Art. 2 HFG

Nach dem Grundsatz der Verhältnismässigkeit darf ein öffentliches Organ Personendaten nur bearbeiten, soweit es zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Wenn es möglich ist, im Rahmen einer Studie eine wissenschaftliche Fragestellung mit anonymisierten Daten zu erforschen, dann sind die Daten vor der Bekanntgabe an das Forschungsinstitut zu anonymisieren. Die Forschung mit anonymisierten gesundheitsbezogenen Daten fällt nicht unter den Geltungsbereich des Humanforschungsgesetzes und kann dadurch einfacher durchgeführt werden.

Automatische Preisfindung mit Smartphone-App

Der Zürcher Verkehrsverbund (ZVV) wandte sich an den Datenschutzbeauftragten mit einem Vorhaben zur automatischen Preisfindung über eine Smartphone-App. Der Datenschutzbeauftragte prüfte das vorabkontrollpflichtige Vorhaben.

Auf der ZVV-App sollen Fahrgäste ihre Fahrt erfassen können, indem sie zu Beginn der Reise einchecken und am Ende wieder auschecken. Das System erfasst die Reise durch Geolokalisierung. Gestützt auf diese Daten wird der Preis berechnet und dem Fahrgast über das hinterlegte Zahlungsmittel belastet. Der ZVV setzt dafür das von der BLS AG entwickelte System Lezzgo ein.

Der Datenschutzbeauftragte hielt fest, dass die Daten, die mit der Nutzung der Funktion in der App erhoben werden, Persönlichkeitsprofile darstellen. Persönlichkeitsprofile sind besondere Personendaten, für deren Bearbeitung das Gesetz höhere Anforderungen verlangt. Der Datenschutzbeauftragte stellte fest, dass ausreichende Rechtsgrundlagen für die Datenbearbeitung vorliegen. Zudem wird der Verhältnismässigkeitsgrundsatz eingehalten, indem nur Personendaten bearbeitet werden, die für die Aufgabenerfüllung geeignet und notwendig sind, und ausschliesslich Mitarbeitende Zugang zu den Personendaten haben, die sie für die Erfüllung ihrer Aufgaben benötigen. Die Aufbewahrungsfrist von einem Jahr erschien dem Datenschutzbeauftragten verhältnismässig. Weiter stellte er fest, dass die Grundsätze der Zweckbindung wie auch der Transparenz ausreichend umgesetzt werden.

Da der ZVV die Bearbeitung der Daten zur automatischen Preisfindung an die BLS AG auslagert, sind die «AGB Datenbearbeitung durch Dritte» als Bestandteil des schriftlich zu schliessenden Vertrags festzuhalten. Der Datenschutzbeauftragte wies darauf hin, dass der Auftragnehmer Dritte zur Erfüllung seines Auftrags nur beiziehen darf, wenn das öffentliche Organ schriftlich zugestimmt hat. Der Unterauftragnehmer muss sämtliche Pflichten aus dem Vertragsverhältnis sowie aus den «AGB Datenbearbeitung durch Dritte» rechtsgültig übernehmen. Die BLS AG darf zudem keine Bewegungsprofile an Dritte weitergeben. Der Datenschutzbeauftragte nahm ausserdem zu organisatorisch-technischen Aspekten des Vorhabens Stellung. Er kam zum Schluss, dass das Vorhaben nach Anpassung der erwähnten Punkte die datenschutzrechtlichen Anforderungen erfüllt.

§ 10 IDG
§ 24 IDV
§ 3 Abs. 4 lit. b IDG
§ 6 IDG
§ 25 IDV

Videoüberwachung in Schulzimmern

Eine Schule wollte im Aufgabenzimmer eine Videokamera installieren, weil Gegenstände entwendet worden waren und die Schülerinnen und Schüler sich gegenseitig Streiche gespielt hatten.

Öffentliche Organe wie Schulen dürfen Personendaten bearbeiten, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben geeignet und erforderlich ist. Im Rahmen des Unterrichts können beispielsweise Videoaufnahmen für pädagogische Zwecke gemacht werden. Zum Schutz von Personen und Sachen kann eine Videoüberwachung eingesetzt werden, wenn dies Teil der Aufgabenerfüllung ist, etwa bei Vandalismus in Schulgebäuden. Das öffentliche Organ muss dabei das Verhältnismässigkeitsprinzip beachten und vor jeder Videoüberwachung prüfen, ob sie zur Erreichung des Zwecks geeignet und erforderlich ist. Es muss abklären, ob mildere Massnahmen, die weniger in die Privatsphäre eingreifen, ausgeschöpft sind und deshalb nur die Videoüberwachung zur Verfügung steht. Wenn alternative Möglichkeiten wie die Klassenaufsicht durch eine Lehrperson möglich sind, dürfen keine Videoaufnahmen gemacht werden.

In einer anderen Schule wurde ein Schüler videoüberwacht, während er einen Leseauftrag in einem separaten Schulzimmer ausführte. Auch in diesem Fall wies der Datenschutzbeauftragte auf den Grundsatz der Verhältnismässigkeit hin. Videoüberwachung sollte nur angewendet werden, wenn keine alternativen Möglichkeiten vorhanden sind wie die Klassenaufsicht durch eine Lehrperson oder das Offenlassen der Zimmertüre. Der Datenschutzbeauftragte geht davon aus, dass höchstens die Übertragung von Bildern in einen anderen Raum zulässig ist, nicht aber die Aufzeichnung. Die Lehrperson übt dann während des Unterrichts in einem anderen Raum die Aufsicht aus und kann bei Bedarf intervenieren.

§ 8 Abs. 1 IDG

Ausweitung der Nutzung der AHV-Nummer

Im Vernehmlassungsverfahren nahm der Datenschutzbeauftragte Stellung zur Frage der Verwendung der AHV-Nummer im Grundbuch. Er hielt fest, dass die Nutzung der AHV-Nummer als Personenidentifikator im Grundbuch abzulehnen ist. Die AHV-Nummer wurde als Sozialversicherungsnummer zur Erleichterung der Koordination im Bereich der sozialen Sicherheit eingeführt. Sie kann den Ansprüchen als Identifizierungsnummer von Personen im Grundbuch nicht gerecht werden, da aufgrund von Mehrfachvergaben von Nummern die Eindeutigkeit nicht gewährt ist. Zudem führt die breite Verwendung der AHV-Nummer in der Verwaltung zu zunehmenden Risiken einer Persönlichkeitsverletzung für die betroffenen Personen. Der Datenschutzbeauftragte schlug die Verwendung eines sektoriellen Personenidentifikators vor, wie dies etwa beim Handelsregister oder beim elektronischen Patientendossier der Fall ist. Weiter äusserte er sich gegen die Errichtung einer zentralen Datenbank, da sie für die Verwendung eines sektoriellen Personenidentifikators nicht nötig ist. Ein sektorieller Identifikator kann wie beim elektronischen Patientendossier in Sekundenfrist durch die Zentrale Ausgleichsstelle (ZAS) generiert werden. Der Einsatz der AHV-Nummer als Personenidentifikator im Grundbuch wäre unverhältnismässig, da er einen übermässigen Eingriff in die Freiheitsrechte der betroffenen Personen darstellt.

Der Regierungsrat liess die Stellungnahme des Datenschutzbeauftragten ausser Acht und führte aus, dass die Verwendung der AHV-Nummer als universellem Personenidentifikator den Datenschutz sogar stärke. Darauf wies der Datenschutzbeauftragte den Regierungsrat auf ein Gutachten von Dr. David Basin, Professor für Informationssicherheit an der ETH, hin. Dieses kam zum Schluss, dass der kontinuierliche Ausbau der AHV-Nummer zum universellen Personenidentifikator mit hohen Risiken für die Grundrechte und die Persönlichkeitsrechte der Bürgerinnen und Bürger verbunden ist. Diese Risiken liessen sich nur reduzieren, wenn sektorspezifische Identifikatoren eingesetzt würden und die Verknüpfung des Identifikators mit den weiteren Personendaten nur über einen gesicherten Prozess erfolgen würde, wie dies beim elektronischen Patientendossier oder beim Handelsregister der Fall ist. Der Datenschutzbeauftragte forderte den Regierungsrat auf, die Überlegungen des Gutachters auf Kantonsebene einzubeziehen und bei den Vorhaben der Digitalisierung sowie bei E-Government-Projekten auf die Verwendung der AHV-Nummer als Personenidentifikator zu verzichten.

§ 8 IDG

Totalrevision Bürgerrechtsverordnung

Die Direktion der Justiz und des Innern überarbeitete im Rahmen einer Totalrevision die Bürgerrechtsverordnung. Auslöser war die Änderung der Rechtsgrundlagen für die Erteilung des Schweizer Bürgerrechts auf Bundesebene. Der Datenschutzbeauftragte nahm im Vernehmlassungsverfahren zu verschiedenen datenschutzrechtlichen Aspekten Stellung.

Er regte an, die Bestimmung über die Veröffentlichung von Einbürgerungen zu ergänzen. Dadurch soll geregelt werden, dass im Internet publizierte Personendaten gelöscht werden müssen, sobald der Zweck der Veröffentlichung erreicht ist. Weiter wies er auf einige Unklarheiten hin. Die Direktion der Justiz und des Innern berücksichtigte die Anmerkungen des Datenschutzbeauftragten und präzisierte einerseits die Ausführungen in der Begründung zur kantonalen Bürgerrechtsverordnung und integrierte andererseits einen Verweis auf bundesrechtliche Regelungen in den Verordnungstext.

Der Datenschutzbeauftragte begrüsst dieses Vorgehen und bringt sein Fachwissen auch im Rahmen der Totalrevision des Gesetzes über das Bürgerrecht ein.

Veranstaltungen

Neue Herausforderungen verlangen neue Regeln

Die digitale Technologie verändert die Gesellschaft. Die Datenschutzgesetze stammen aus einer Zeit, in der die heutigen Entwicklungen kaum vorstellbar waren. An zwei Veranstaltungen diskutierten Praktikerinnen und Praktiker wie auch Expertinnen und Experten darüber, wie die rechtliche und soziale Zukunft gestaltet werden könnte.

Am 3. Mai 2017 lud der Datenschutzbeauftragte ein, um auf zehn Jahre Erfahrungen mit dem Gesetz über die Information und den Datenschutz (IDG) zurückzublicken sowie die aktuellen technologischen und rechtlichen Entwicklungen und die Anforderungen an die schweizerische und vor allem die kantonale Gesetzgebung zu diskutieren. An der Veranstaltung «Herausforderungen der Digitalisierung und gesetzgeberische Entwicklungen» wurde den rund 150 Teilnehmenden aus der kantonalen Verwaltung, aus Gemeinden und anderen öffentlichen Organen klar, dass die Digitalisierung die Rahmenbedingungen grundlegend verändert. Die Digitalisierung könne den Zugang der Bürgerinnen und Bürger zu den Diensten der Verwaltung erleichtern, sie bringe aber auch neue Risiken. Es müsse alles daran gesetzt werden, dass das Vertrauen der Bürgerinnen und Bürger in die Datenbearbeitungen der Verwaltung erhalten bleibe, meinte der scheidende Präsident des Kantonsrates, Rolf Steiner.

Mit dem IDG sei ein Paradigmenwechsel herbeigeführt worden, indem vor zehn Jahren der Zugang zu und der Schutz von Informationen in einem Gesetz geregelt wurden. Die Daten seien inzwischen mobil geworden. Deshalb müssten die Anstrengungen für die Sicherheit und den Schutz der Daten erhöht werden, verlangte der Datenschutzbeauftragte. Die Stadtschreiberin von Schlieren, Ingrid Hieronymi, forderte, dass auch in Zukunft auf Gebühren für den Informationszugang zu verzichten sei, denn der Aufwand sei im Verhältnis zum Nutzen für die Bürgerinnen und Bürger gering. In den weiteren Referaten zeigte Peppino Giarritta, Leiter E-Government Kanton Zürich, die Perspektiven der Digitalisierung der Verwaltung auf, während der Datenschutzdelegierte der Universität Zürich, Robert Weniger, die Entwicklungen beim europäischen Recht präsentierte.

Für Regierungsrätin Jacqueline Fehr bieten die anstehenden Revisionen auf europäischer, eidgenössischer und kantonaler Ebene die Chance, einen markanten Schritt in Richtung verstärkte Bürgerrechte zu gehen.

Sensitive Daten für alle?

Das 22. Symposium on Privacy and Security Ende August suchte nach Lösungen, wie sensitive Daten in Zukunft bearbeitet werden können, während der Schutz der Privatheit gewährleistet bleibt.

Seit über zwei Jahrzehnten werden am Symposium im Spätsommer einen Tag lang aktuelle Herausforderungen in Informationssicherheit und Datenschutz durch nationale und internationale Referentinnen und Referenten vertieft. Rund 200 Vertreterinnen und Vertreter aus der Verwaltung, den Gemeinden und privaten Organisationen nehmen jeweils teil.

Im Jahr 2017 wurden die Herausforderungen der Öffnung und Vernetzung der Silos mit sensitiven Daten beleuchtet. In seiner Übersicht der Entwicklungen im Bereich Quantified Self, der Selbstvermessung mit sogenannten Wearables wie Fitness Trackern, kam Hermann Kollmar von Medgate zum Schluss, dass sinnvolle Regeln für die neue Technologie geschaffen werden müssen. Die Kontrolle dürfe nicht abgegeben werden. Bei Gesundheitsdaten sei eine Sozialpflichtigkeit, also eine Bürgerpflicht, die Daten zur Verfügung zu stellen, nicht vereinbar mit unserer Rechtsordnung, die den Menschen als freies und selbstbestimmtes Wesen definiere und sich an demokratischen und rechtsstaatlichen Grundwerten orientiere, meinte die Juristin Franziska Sprecher.

Datenschutzfreundliche soziale Medien sind möglich

Der Publizist und Jurist Milosz Matuschek nutzte die Carte Blanche am Symposium on Privacy and Security, um die Datensammlung der digitalen Welt aus einem gesellschaftlichen Blickwinkel zu betrachten. Das Smartphone sei die Maschine, mit der Personendaten der Menschen gemolken würden. «Wir sind dümmer als die Kühe, wir bezahlen sogar noch für die Melkmaschine», meinte er. In drei kurzen Videos des Datenschutzbeauftragten entwickelt Matuschek Perspektiven zum Verhalten im Internet, zum Umgang mit sozialen Medien und dazu, wie eine datenschutzfreundliche weitere Entwicklung möglich wäre. Die Videos eignen sich als Einstieg zu Workshops und Diskussionen.

Youtube-Kanal des Datenschutzbeauftragten

Kontakt

E-Mail	datenschutz@dsb.zh.ch
Adresse	Datenschutzbeauftragter des Kantons Zürich, Postfach, CH-8090 Zürich
Internet	www.datenschutz.ch
Twitter	twitter.com/dsb_zh
Youtube	www.youtube.com/channel/UCghVVLU_hOTbClYaKQk8hTw
Telefon	+41 43 259 39 99

Impressum

Herausgeber	Datenschutzbeauftragter des Kantons Zürich, Postfach, 8090 Zürich
Korrektorat	Text Control, Im Struppen 11, 8048 Zürich
Grafik	TKF Kommunikation & Design, t-k-f.ch

Der Tätigkeitsbericht 2017 ist elektronisch verfügbar unter
www.datenschutz.ch/TB2017.

ISSN 2571-5003

Datenschutz mit Qualität

datenschutz.ch