dsb

datenschutzbeauftragter
kanton zürich

Tätigkeitsbericht 2019

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 2019 bis und mit 31. Dezember 2019 ab und wird auch im Internet unter www.datenschutz.ch veröffentlicht.

Der Tätigkeitsbericht 2019 ist der 25. und zugleich der letzte in meiner Amtszeit. Ich will allen danken, die während meiner Amtszeit zur Entwicklung des Datenschutzes und der Informationssicherheit im Kanton Zürich beigetragen haben. Die positive Unterstützung wie auch die kritischen Auseinandersetzungen haben ermöglicht, dass der persönlichen Freiheit und der Selbstbestimmung der Bürgerinnen und Bürger auch bei der Digitalisierung der Verwaltung ein hoher Stellenwert zukommt.

Ich wünsche meiner Nachfolgerin, Dr. Dominika Blonski, und allen Mitarbeitenden, dass sie weiterhin auf dieses Wohlwollen der öffentlichen Organe im Kanton Zürich zählen können.

Zürich, im März 2020

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

Fit für die Digitalisierung

Cloud Computing ist ein Trend, auf den auch die Verwaltung im Laufe der fortschreitenden Digitalisierung setzt. Sie beinhaltet besondere Risiken für den Datenschutz und die Datensicherheit. Mit den zusätzlichen Ressourcen wird der Datenschutzbeauftragte in Zukunft datenschutzkonforme Lösungen mitgestalten können.

Das Cloud Computing entwickelt sich für die öffentlichen Organe zu einem Kernthema. Viele neue Anwendungen nutzen die Cloud mindestens teilweise und so fliessen Daten und Datenbearbeitungen immer weiter von der bearbeitenden Stelle weg. In der Cloud werden die Ressourcen für die Datenbearbeitungen dynamisch zur Verfügung gestellt und eine konkrete Lokalisation von Datenbearbeitungen und Daten ist nicht vorgesehen: Die Daten befinden sich eben in der Cloud. Die öffentlichen Organe tragen aber weiterhin die volle Verantwortung für den Datenschutz und die Datensicherheit. Daraus ergeben sich grosse Herausforderungen. Der Datenschutzbeauftragte unterstützte die Verwaltung dabei in verschiedenen Projekten.

Viele cloudbasierte Anwendungen sind als Standardprodukte konzipiert. Ihre rechtlichen Rahmenbedingungen werden durch Allgemeine Geschäftsbedingungen des Anbieters definiert. Sie sehen oft ausländisches Recht und einen ausländischen Gerichtsstand vor. Dies erschwert dem öffentlichen Organ die Rechtsanwendung und -durchsetzung. Es hat zu vereinbaren, dass die Rahmenbedingungen des kantonalen Gesetzes über die Information und den Datenschutz (IDG) umzusetzen sind und der Gerichtsstand in der Schweiz liegt. In Verhandlungen mit den Anbietern Apple, Google und Microsoft ist es für den Bildungsbereich gelungen, diese Bedingungen in Standardverträgen zu integrieren. Für die allgemeine Verwaltung gelten andere Verträge. Sie müssen neu verhandelt werden (Seite 20).

Weitere Fragen stellen sich bei Daten, die unter dem Berufsgeheimnis im Gesundheitsbereich oder einem Spezialgeheimnis stehen, beispielsweise dem Steuergeheimnis oder dem Sozialhilfegeheimnis. Dafür lässt sich ein angemessener Schutz der Daten nur mit organisatorischen und technischen Massnahmen erreichen. Beim Berufsgeheimnis wäre dies durch eine Verschlüsselung und dem Schlüsselmanagement beim öffentlichen Organ möglich. Damit wird aber die Funktionalität einer Cloud eingeschränkt.

In diesem Zusammenhang ist auch zu berücksichtigen, wie weit ausländische Behörden auf Daten in der Cloud zugreifen können, ohne ein Rechtshilfeverfahren einzuleiten. Dies ist heute zum Beispiel bei US-Firmen der Fall, die dem CLOUD Act[1] unterliegen.

Die Fragen rund um den Datenschutz und die Datensicherheit in der Cloud zeigen einen Handlungsbedarf, der in einer Cloud-Strategie der öffentlichen Organe aufgenommen werden und konkret reguliert werden sollte. Dabei wären auch weitere Risiken wie die Abhängigkeit von fremden Infrastrukturen zu berücksichtigen.

[1] Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

Infrastrukturen, die durch andere Organisationen betrieben werden, bergen hohe Risiken für die Daten. Dies gilt auch für die föderierte Infrastruktur zur Verwaltung von elektronischen Identitäten im Bildungsbereich, FIDES respektive Edulog genannt. Der Datenschutzbeauftragte prüfte für die Bildungsdirektion die geplante Infrastruktur mit einer Vorabkontrolle (Seite 18). Die Verantwortung für die Plattform liegt bei der Fachabteilung Educa.ch der Erziehungsdirektorenkonferenz (EDK). Ihr Betrieb ist vollständig an Educa.ch ausgelagert. Die Daten fliessen aus dem kantonalen Bildungsbereich an Educa.ch und von hier weiter an die Dienstleistungsanbieter im Bildungsbereich. Deshalb ist darauf zu achten, dass nur Daten bearbeitet werden, die für den Betrieb geeignet und erforderlich sind. Der Datenschutzbeauftragte hat die rechtlichen Rahmenbedingungen geprüft und gab verschiedene Hinweise, wie ein datenschutzkonformer Betrieb sichergestellt werden kann. Educa.ch sicherte zu, diese Hinweise umzusetzen.

Internationale Datenschutz-Auszeichnung für den Kanton Zürich

Der Datenschutzbeauftragte erhielt 2019 den Global Privacy and Data Protection Award für das Lehrmittel «Geheimnisse sind erlaubt», das er zusammen mit der Pädagogischen Hochschule Zürich (PHZH) entwickelte. Der Global Privacy and Data Protection Award ist der international bedeutendste fachspezifische Preis und wird von der Internationalen Konferenz der Datenschutzbeauftragten, der Global Privacy Assembly, vergeben. An der Konferenz tauschen sich jährlich über 800 Fachleute aus allen Kontinenten aus. «Der Global Privacy and Data Protection Award honoriert kreative Ideen, praktische Innovationen und die hervorragenden Menschen, die zu unserer Gemeinschaft gehören», sagte die Präsidentin der Konferenz, Elizabeth Denham, an der Preisverleihung. Es sei nicht nur ein Preis, sondern eine Anerkennung durch Fachkolleginnen und Fachkollegen.

Das ausgezeichnete Lehrmittel ist weltweit einzigartig. Für das Projektteam aus Mitarbeitenden des Datenschutzbeauftragten und der PHZH lag die Herausforderung darin, die komplexen Themen der Privatsphäre und des Datenschutzes für die kleinsten Schulkinder begreifbar zu machen. In fünf Modulen lernen sie, dass es Geheimnisse gibt, die man für sich behalten soll, während andere mit den Eltern oder einer anderen erwachsenen Vertrauensperson geteilt werden sollen. Sie begreifen, wie sie ohne Geheimnisse manipulierbar werden und ihre Freiheit eingeschränkt wird. Durch den Einsatz einer Vielfalt didaktischer Methoden kann das Lehrmittel in unterschiedlichen Umfeldern eingesetzt werden. Die Kinder entdecken dadurch, wie wichtig der Schutz der Privatsphäre für die verschiedenen Lebensbereiche ist. Die online frei verfügbaren Unterrichtsmaterialien sind integraler Bestandteil der Lehrpersonenausbildung an der PHZH.

Die erfolgreiche Zusammenarbeit des Datenschutzbeauftragten mit der PHZH wird weitergeführt. Das Projektteam erarbeitet Lerninhalte für die Zyklen 2 und 3 des Lehrplans 21. Die Schülerinnen und Schüler sollen sich innerhalb der obligatorischen Schulzeit die Kompetenzen aneignen können, mit denen sie in den ständig neuen Lebenssituationen der rasanten digitalen Entwicklung eine selbstbestimmte Haltung einnehmen und ihre Privatsphäre und die der anderen wirksam schützen können.

Gemeinden lassen viele Anwendungen von Dritten betreiben. Der Datenschutzbeauftragte setzte die Kontrollen bei den Auftragnehmern fort. Die Prüfungen stossen auf ein positives Echo nicht nur bei den Auftragnehmern, sondern auch bei den Gemeinden. Die Kontrollen stellen sicher, dass Mängel breitflächig behoben werden. Wenn ein Auftragnehmer den Sicherheitsstandard verbessert, profitieren alle Gemeinden davon, die zu seiner Kundschaft gehören. 2019 konnte zudem ein neues Kontrollkonzept für die Gemeinden entwickelt werden, mit dem die Wirkung der Kontrollen vergrössert wird (Seite 27). Die Kontrollen der Auftragnehmer tragen zu einem besseren Sicherheitsniveau bei den Gemeinden bei, das als Fundament für die neuen Digitalisierungsprojekte dienen kann.

Das Impulsprogramm zur Digitalisierung der kantonalen Verwaltung entwickelte im abgelaufenen Jahr eine grosse Dynamik. Der Datenschutzbeauftragte ist auf der operativen Ebene in die wichtigen Projekte involviert und freut sich darüber, dass sich die Zusammenarbeit in den verschiedenen Bereichen gut entwickelt. In den vielen offenen rechtlichen, organisatorischen und technischen Fragen ist eine Lösungsfindung aufgegleist, die auch den Datenschutz und die Datensicherheit berücksichtigt.

Die bisherigen Ressourcen verhinderten, dass der Datenschutzbeauftragte mit der Dynamik der Digitalisierungsprojekte mithalten konnte. Er konnte verschiedentlich nicht oder nicht rechtzeitig auf Anforderungen der Verwaltung reagieren. Die rasante Entwicklung wird in absehbarer Zeit nicht abnehmen. Vielmehr ist damit zu rechnen, dass die Anzahl der behandelten Geschäfte durch die Digitalisierung bei den Gemeinden und den übrigen öffentlichen Organen weiter zunimmt. Für die Digitalisierung der Verwaltung wäre es fatal, wenn Fragen des Datenschutzes und der Datensicherheit unbearbeitet blieben. Der Kantonsrat sah dies ebenso und stimmte deshalb in der Budgetdebatte einer Aufstockung der Ressourcen beim Datenschutzbeauftragten zu. Damit wird auch die Behörde des Datenschutzbeauftragten fit für die Digitalisierung.

Mehr Wirkung erzielt

Der Konsolidierte Entwicklungs- und Finanzplan (KEF) des Datenschutzbeauftragten enthält neben den Leistungsindikatoren auch zwei Wirkungsindikatoren. Ihre Entwicklung weist auf gelungene Umsetzungsmassnahmen hin.

Im Rahmen der Datenschutzreviews gibt der Datenschutzbeauftragte dem öffentlichen Organ Hinweise, mit welchen Massnahmen Mängel im rechtlichen, organisatorischen und technischen Bereich zu beheben sind. Für ihre Umsetzung wird eine Frist von bis zu zwölf Monaten angesetzt. In der Vergangenheit haben sich zahlreiche öffentliche Organe nicht oder zu wenig um die Umsetzung der Massnahmen gekümmert. Der Datenschutzbeauftragte hat deshalb entschieden, vermehrt Nachkontrollen durchzuführen und bei mangelnder Umsetzung der Massnahmen einen Bericht einzufordern. Aktuell werden immer noch nur etwa 66 Prozent der Massnahmen umgesetzt. Trotzdem ist dies eine deutliche Steigerung gegenüber dem Vorjahr, in dem 47 Prozent der Massnahmen umgesetzt wurden. Die Nachkontrollen des Datenschutzbeauftragten zeigen also Wirkung. Mittelfristig gilt es, das KEF-Ziel beizubehalten und längerfristig zu erhöhen, sofern mehr Nachkontrollen durchgeführt werden können.

Die Anzahl der Besuche auf unserer Website ist ein weiterer Wirkungsindikator. Er weist auf die Qualität des Informationsangebots des Datenschutzbeauftragten hin. Die Nutzerinnen und Nutzer sind hauptsächlich Mitarbeitende der öffentlichen Organe. Sie suchen aktuelle Informationen zu Datenschutz und Informationssicherheit. Sie nutzen das Angebot, wenn es ihren Ansprüchen entspricht. Die Website ist deshalb inhaltlich kontinuierlich weiterzuentwickeln, um aktuell und informativ zu bleiben. Der Indikator weist darauf hin, dass die Nachfrage konstant ansteigt und damit die Bedürfnisse der Nutzerinnen und Nutzer durch das Informationsangebot qualitativ und quantitativ gut abgedeckt wird.

Die beiden Leistungsindikatoren Anzahl Beratungen und Anzahl Kontrollen zeigen die angespannte Ressourcensituation. Die Anzahl Beratungen liegt konstant über der eigentlichen Kapazität von 500 Beratungen pro Jahr. Die Qualität der Beratungen und deren zunehmende Anzahl kann nur mit zusätzlichen Ressourcen sichergestellt werden. Das Ziel von 40 Kontrollen pro Jahr konnte mangels Ressourcen nicht erreicht werden.

Mit den vom Kantonsrat im Budget 2020 bewilligten zusätzlichen Ressourcen wird es möglich sein, diese KEF-Ziele mittelfristig zu erreichen.

		KEF	2017	2018	2019
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	600	**657**
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	25	**30**
Massnahmenumsetzung	Der DSB gibt im Rahmen der Datenschutzreviews dem öffentlichen Organ Hinweise, mit welchen Massnahmen Mängel im rechtlichen, organisatorischen und technischen Bereich zu beheben sind. Der Wirkungsindikator im KEF misst die prozentuale Umsetzung der Massnahmen durch die kontrollierten Organe.	**60 %**	42 %	47 %	**66 %**
Website-Besuche	Der DSB stellt auf seiner Website Informationen zu Datenschutz und Informationssicherheit zur Verfügung. Die Nutzerinnen und Nutzer sind hauptsächlich Mitarbeitende der öffentlichen Organe. Der Wirkungsindikator im KEF gibt Auskunft über die Nutzung der Informationsangebote.	**45 000**	31 575	42 570	**47 618**

Mit klarem Kopf in der Cloud

Mit klarem Kopf in der Cloud

Cloud Computing vereinfacht viele Prozesse. Im Vergleich mit der herkömmlichen Auslagerung eröffnet Cloud Computing neue Welten der Datenbearbeitung. Auch die Verwaltung möchte davon profitieren, allen voran der Bildungsbereich.

Im Berichtsjahr erhielt der Datenschutzbeauftragte eine grosse Anzahl Anfragen zum Thema Cloud Computing. Die zur Prüfung vorgelegte Produktepalette ist riesig, betrifft unterschiedliche Anbieter und alle Bereiche der Verwaltung. Einige Überlegungen sind jedoch gleich, unabhängig davon, ob es sich um das Produkt eines grossen Anbieters oder einer kleinen Spezialfirma handelt.

Zuerst stellt sich die Frage nach der Art der Daten und nach den Geheimnispflichten, denen die Daten unterliegen. Hier entscheidet sich, welche Massnahmen durch den Anbieter und das öffentliche Organ umgesetzt werden müssen. Dazu gehören technische Massnahmen wie die Verschlüsselung, die Trennung von Mandanten in der Cloud oder die Portabilität der Daten und organisatorische Massnahmen wie ein Back-up oder ein Passwortkonzept. Mit diesen Massnahmen lässt sich der Transparenz- und Kontrollverlust minimieren, der mit dem Cloud Computing einhergeht. Der Datenschutzbeauftragte hat auf seiner Website detaillierte Dokumente veröffentlicht, die bei der Bestimmung der notwendigen Massnahmen helfen.

In der Praxis scheitern viele Projekte daran, dass die Massnahmen zur Informationssicherheit gar nicht umgesetzt werden können. Die Verschlüsselung der Daten während des Transports und in der Cloud selber erhöht die Sicherheit umfassend. Oft ist sie möglich, verhindert jedoch, dass alle Funktionalitäten eines Produkts ausgeschöpft werden können. Weiter stellt sich die Frage, ob der Schlüssel für die verschlüsselten Daten beim öffentlichen Organ liegt. Ist dies beispielsweise aus technischen Gründen nicht möglich, dürfen etwa Berufsgeheimnisdaten nicht durch Anbieter bearbeitet werden, die dem US-amerikanischen CLOUD Act unterliegen.

Oft verhindert die mangelnde Flexibilität von Anbietern, dass ein Produkt genutzt werden kann, etwa wenn sie sich weigern, ihre Verträge datenschutzkonform auszugestalten. Für öffentliche Organe gilt aber, dass beim Auslagern von Personendaten schweizerisches Recht anzuwenden und ein schweizerischer Gerichtsstand zu vereinbaren ist.

Die öffentlichen Organe müssen unter Abwägung aller relevanten Faktoren im Rahmen einer sorgfältigen Risikoanalyse entscheiden, ob bezüglich einer spezifischen Datenbearbeitung Cloud Computing in Anspruch genommen werden kann. Der Datenschutzbeauftragte bietet ihnen seine Unterstützung an.

Apple, Google, Microsoft & Co.

Der Datenschutzbeauftragte hat mit den grossen Anbietern Kontakt aufgenommen, um allen Schulen die gleichen datenschutzkonformen Bedingungen zu ermöglichen bei der Nutzung der marktbeherrschenden Produkte. Google G Suite for Education wird 2020 von den Schulen datenschutzkonform genutzt werden können. Dies trifft ebenfalls für das Produkt School Manager von Apple zu. Die Rahmenverträge für den Einsatz von Office 365 werden durch Educa.ch und Switch neu verhandelt.

Für die Nutzung dieser Dienstleistungen werden durch den Datenschutzbeauftragten neue Leitfäden erarbeitet. Die Schulen erfahren daraus, welche Verträge unterzeichnet werden müssen, welche Vorarbeiten zu tätigen und welche Massnahmen während der Nutzung des Produkts umzusetzen sind.

Der Datenschutzbeauftragte beantwortet weiterhin offene Fragen bei der Umsetzung und informiert regelmässig, wenn neue Dokumente zu diesen Themen publiziert werden.

Vielfalt digitaler Tools in den Schulen

Im Schulbereich werden zunehmend digitale Produkte und Cloud-Dienste eingesetzt. Eltern und Lehrpersonen aus verschiedensten Schulstufen melden sich beim Datenschutzbeauftragten und fragen nach Hilfestellungen. Die datenschutzrechtliche Prüfung dieser Produkte ist oft äusserst komplex.

Eine Schule darf Daten nur für die Zwecke bearbeiten, die zur Aufgabenerfüllung notwendig sind. Dies gilt auch, wenn mehr Daten als notwendig vorhanden sind und Auswertungen für andere Zwecke möglich wären. Der Datenschutzbeauftragte hat in seiner Beratungstätigkeit darauf aufmerksam gemacht, dass mit einem unkontrollierten Einsatz von digitalen Produkten Persönlichkeitsprofile entstehen. Persönlichkeitsprofile beinhalten ein hohes Missbrauchspotenzial. Eine Lehrperson kann beispielsweise mithilfe von eingesetzten Produkten feststellen, zu welcher Uhrzeit eine lernende Person welche Aufgaben gemacht hat oder wie lange sie für welche Aufgaben gebraucht hat. Sie kann daraus ableiten, ob eine Person die ganze Nacht wach war. Diese Auswertung der vorhandenen Daten ist nicht erlaubt.

Schultablets zu Hause nutzen

Ein Vater wandte sich an den Datenschutzbeauftragten, da in der Primarschule seiner Töchter Tablets eingeführt wurden. Mit den Tablets stieg auch die Zahl der benutzten digitalen Unterrichtswerkzeuge, wie Internetplattformen zum Vokabellernen oder zum Protokollieren der Hausaufgaben. Der Datenschutzbeauftragte hatte einige der fraglichen Produkte schon geprüft und befunden, dass sie datenschutzkonform genutzt werden können. Dafür muss die Schule Rahmenbedingungen definieren. Die Auswertung von Protokollen und Analysen der Daten muss immer der Zweckerfüllung der Schule dienen. Mit der Abgabe von Tablets stellen sich in der Praxis allerdings Fragen zu den Benutzerrechten, etwa dazu, wer welche Daten löschen darf. Wann darf die Schülerin oder der Schüler welche Daten löschen? Welche Daten darf die Lehrperson löschen? Bei den Eltern herrscht oft Unsicherheit oder ein unbehagliches Gefühl. Die Eltern sind einzubeziehen und über die Regeln beim Einsatz der Instrumente zu informieren.

Risikoanalyse bei Cloud-Diensten

Der Datenschutzbeauftragte prüfte einzelne schulrelevante Cloud-Dienste. Für die Prüfung von Verträgen mit Dienstleistern stellt der Datenschutzbeauftragte auf seiner Website den Leitfaden Bearbeiten im Auftrag zur Verfügung. Oft stellen die Anbieter den Schulen nicht einmal die notwendigen Informationen und Unterlagen zur Verfügung, um die Online-Dienste datenschutzrechtlich beurteilen zu können. Bei jedem Produkt muss zunächst festgestellt werden, welche Daten zu welchem Zweck ausgelagert werden. Die Schule muss den Gerichtsstand und das anzuwendende Recht abklären. Der Datenschutzbeauftragte rät anhand einer Risikoanalyse, die zu protokollierenden Informationen zu definieren, die Protokollierung von Änderungen zu regeln und angemessene Aufbewahrungsfristen festzulegen.

Lernplattformen, Umfragetools und Blogs

Auf der Stufe der Berufsschulen behandelte der Datenschutzbeauftragte Anfragen zum Einsatz von Produkten wie digitale Lernplattformen, Umfragetools oder Blogs. Die Schulen wünschten digitale Gruppenarbeitsräume.

Wenn Lernplattformen von den Schulen selbst betrieben werden, müssen diese die Informationssicherheit gewährleisten können. Werden für den Betrieb Dritte beauftragt, müssen die Voraussetzungen für eine Auslagerung erfüllt sein. Dazu müssen der Gerichtsstand, anwendbares Recht, Informationssicherheitsmassnahmen inklusive Informationen zur Speicherung und Löschung der Daten geprüft werden.

Vor der Nutzung ist in einem Konzept festzulegen, wer wann was macht. Der Datenschutzbeauftragte rät dazu, die Plattformen wenn möglich anonymisiert oder pseudonymisiert zu nutzen. Die Lernenden sind über mögliche Auswertungen zu informieren. Der Umfang der Datenbearbeitung bei der Nutzung von Lernplattformen oder Blogs ergibt sich durch den schulischen Auftrag. Schulen dürfen nur die Daten erheben und bearbeiten, die für die Aufgabenerfüllung der Schule erforderlich sind.

Bring Your Own Device

Für den Berufsfachschulunterricht hielt der Datenschutzbeauftragte fest, dass die Schülerinnen und Schüler auf freiwilliger Basis private Geräte verwenden dürfen. Dafür müssen die minimalen Schutzmassnahmen eingehalten werden. Diese umfassen die Einrichtung eines Passwortschutzes, die Installation eines Virenschutzprogramms, eine aktuelle Firewall sowie die Durchführung regelmässiger System-Updates und die Verschlüsselung sensitiver Daten bei der Speicherung und Übermittlung. Unter diesen Voraussetzungen hiess der Datenschutzbeauftragte auch die lokale Installation von Programmen wie Teams oder Onenote gut.

Ja zu digitalen Lehrmitteln und Lernfördersystemen

Lehr- und Lernprozesse mit digitalen Lehrmitteln und digitalen Lernfördersystemen gewinnen in der Volksschule an Bedeutung. Das Volksschulamt (VSA) und der Lehrmittelverlag Zürich (LMVZ) richteten diverse Fragen zu digitalen Lehrmitteln und Lernfördersystemen an den kantonalen Datenschutzbeauftragten.

Der Datenschutzbeauftragte analysierte mit den Verantwortlichen von VSA und LMVZ die Ausgangslage und mögliche Szenarien in Bezug auf die Datensicherheit, den Schutz der Privatsphäre sowie die Profilbildung. Die organisatorischen Rahmenbedingungen zum datenschutzkonformen Einsatz von digitalen Lehrmitteln wurden ebenso erörtert wie Fragen zu problematischen Datensammlungen. Besonderes Augenmerk fiel auf die technischen Möglichkeiten, vorhandene Datenbestände zu aggregieren, diese Verbindungen zu analysieren und daraus Schlussfolgerungen zu ziehen. Ähnliche Auswertungen wären vor der Digitalisierung zwar schon möglich gewesen, wurden aber aufgrund des manuellen und personellen Aufwands nicht umgesetzt.

In gedruckten Lehrmitteln erarbeiteten Schülerinnen und Schüler Aufgaben, die von den Lehrpersonen korrigiert und beurteilt wurden. Digitale Lehrmittel sollen in gleichem Masse genutzt werden können. Dazu benötigen die Lehrpersonen Einblick in die Nutzungsdaten der Lernenden. Die bisherige strikte Trennung von Nutzer- und Nutzungsdaten bei digitalen Lehrmitteln soll dafür aufgeweicht werden. Der Paradigmenwechsel führt zu zusätzlichen Datenbearbeitungen, insbesondere durch die Lehrpersonen in Bezug auf die Schülerinnen und Schüler.

Digital fallen oft mehr Daten an als bei einer Datenbearbeitung in analoger Form. Bei der analogen Hausarbeit hat die Lehrperson in der Regel keine genauen Informationen über Tag und Uhrzeit oder Dauer der Aufgabenbearbeitung, ebenso wenig darüber, wie oft eine Schülerin oder ein Schüler die Arbeiten unterbrochen hat. Bei digitalen Lehrmitteln werden diese Randdaten protokolliert. Die Schule muss sich vor dem Einsatz Gedanken machen über die Art und Weise der Nutzung digitaler Instrumente. Daten, die für den Lehrauftrag nicht notwendig sind, müssen in den Systemeinstellungen ausgeblendet oder sofort gelöscht werden. Der permanente Zugriff auf die Lernergebnisse durch die Lehrperson ist nicht erlaubt. Eltern, Schülerinnen und Schüler sowie Lehrpersonen sind vor dem Einsatz der digitalen Lehrmittel über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung der Daten zu informieren.

Eindeutiger Identifikator für den Bildungsraum Schweiz

Die Bildungsdirektion bat den Datenschutzbeauftragten, die von der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) vorgeschlagene Föderation von Identitätsdiensten für den Bildungsraum Schweiz (FIDES) zu prüfen. Die Identifizierungs- und Zugangsmanagement-Lösung für das Schweizer Bildungssystem ist heute unter dem Namen Edulog bekannt und wird durch Educa.ch angeboten.

Edulog soll den sicheren und transparenten Zugang der Volksschulen und der Sekundarstufe II zu verschiedenen Dienstleistern gewährleisten, beispielsweise dem Lehrmittelverlag. Die zentrale Föderationsplattform soll zukünftig die einzelnen Schulen als Identitätsanbieterinnen einbinden und ihnen die Verantwortung und Kontrolle über ihre Daten belassen. Der Datenschutzbeauftragte beurteilte die Plattform in einer Vorabkontrolle.

Die Verantwortlichen stützten die Datenbearbeitungen im Rahmen des Projekts auf das Konkordat über die Schulkoordination sowie auf ein spezifisches Organisationsreglement. Das Projekt erwies sich als komplex. Die Datenbearbeitungen durch die Föderationsplattform mussten von denjenigen durch die Schule und durch die Dienstleister unterschieden werden. Die Vorabkontrolle ergab, dass die geplante Datenbearbeitung keine genügende Rechtsgrundlage hatte. Die Datenbearbeitungen waren ungenügend beschrieben und es war nicht klar ersichtlich, bei wem die datenschutzrechtliche Verantwortung für welche Daten und ihre Bearbeitung liegen würde.

Aufgrund des Resultats der Vorabkontrolle wurde das Organisationsreglement angepasst, etwa betreffend die Zweckbindung und die Klarheit der Bestimmungen. Das Verhältnismässigkeitsprinzip wurde stärker berücksichtigt und nicht notwendige Datenbearbeitungen eliminiert. Edulog genügt damit den datenschutzrechtlichen Anforderungen, auch im Sinne einer Übergangslösung bis zu einer Revision des Konkordats.

Die Datenschutz- und Informationssicherheits-Managementsysteme von Edulog sollen zukünftig nach ISO 27001 und Good Privacy zertifiziert werden. Dadurch sind die generellen Informationssicherheitsanforderungen sichergestellt. Im organisatorisch-technischen Bereich gibt es Optimierungsbedarf bei den Prozessen für die Generierung, Erstverwendung, Änderung und Löschung einer Identität. Der Datenschutzbeauftragte wies darauf hin, dass bestehende Standards für die Föderation von Identitäten zu verwenden sind.

Der intensive Dialog und der aktive Miteinbezug von Educa.ch in die Beurteilung ermöglichte, das Projekt datenschutzkonform umzusetzen.

Plagiate mit einer Software erkennen

Eine Hochschule möchte eine Software einsetzen, um Abschlussarbeiten auf Plagiate zu überprüfen. Sie legte das Projekt dem Datenschutzbeauftragten zur Vorabkontrolle vor.

Zur Nutzung dieser Software müssten die Studierenden beim Softwareanbieter ein Benutzerkonto mit Name, Vorname und E-Mail-Adresse einrichten. Die Arbeiten würden beim Anbieter gespeichert. Die Nutzung der Software wäre freiwillig und würde auf der Einwilligung der Studierenden basieren.

Der Datenschutzbeauftragte kam in der Vorabkontrolle zum Schluss, dass ein solches Vorhaben einer Hochschule nicht freiwillig sein kann. Die Hochschule muss über eine gesetzliche Grundlage verfügen. Die Nutzung der Software gestützt auf eine Einwilligung ist nicht möglich. Das IDG sieht ein Bearbeiten von Personendaten mit Einwilligung nicht vor. Beim Einsatz dieser Software handelt es sich um eine Auftragsdatenbearbeitung. Die Hochschule bleibt für die Datenbearbeitung durch den Software-Anbieter verantwortlich.

Der Software-Anbieter war dem Swiss-US Privacy Shield beigetreten und die Standardvertragsklauseln waren Bestandteil des Vertragspakets. Dadurch verfügt er über ein angemessenes Datenschutzniveau. In den Verträgen waren auch die Datenkategorien, die Zweckbindung, die Rechte der Betroffenen, die Kontrollmöglichkeit der Hochschule, die Anwendbarkeit von schweizerischem Recht und ein schweizerischer Gerichtsstand festgehalten.

Der Datenschutzbeauftragte riet der Hochschule, nur die für eine Plagiatsüberprüfung notwendigen Personendaten an den Anbieter zu übermitteln. Dafür sollte nur ein Benutzerkonto durch die Hochschule eröffnet werden, über das die Arbeiten geprüft werden könnten. Weiter ist durch die Hochschule zu prüfen, wie die Arbeiten der Studierenden anonymisiert oder pseudonymisiert werden können.

Office 365 für die Verwaltung

Der Datenschutzbeauftragte wurde von Anfragen überhäuft, ob Office 365 nicht nur in Schulen, sondern auch in der Verwaltung eingesetzt werden könne. Ein Amt fragte an, wie eine Ausschreibung für die neue Ausstattung von Arbeitsplätzen zu gestalten sei.

Das öffentliche Organ bleibt immer verantwortlich für seine Daten, auch wenn es Produkte mit Cloudnutzung einsetzt, beispielsweise Office 365. Dies ist die Ausgangslage für alle Überlegungen. Wie kann diese Verantwortung wahrgenommen werden? Erstens muss der Vertrag datenschutzkonform sein. Er muss die gesetzlichen Anforderungen erfüllen, schweizerisches Recht für anwendbar erklären sowie einen schweizerischen Gerichtsstand festhalten. Zweitens müssen die Sicherheitsmassnahmen vorgesehen sein, die der Art und dem Umfang der Datenbearbeitung entsprechen. Drittens muss das öffentliche Organ beispielsweise ein Konzept erarbeiten, aus dem hervorgeht, wie welche Dienste mit welcher Art von Daten zu welchem Zweck genutzt werden. Bei der Nutzung sind teilweise Speicherorte und Verschlüsselungsmechanismen auszuwählen oder Lösch- und Protokollierungsfunktionen einzustellen.

Mit einer Gesamtrisikoanalyse ist zu bestimmen, ob ein Produkt in Anspruch genommen werden kann. Sind beispielsweise Berufsgeheimnisdaten betroffen, kann eine Auslagerung aufgrund hoher Risiken für die Persönlichkeitsrechte eingeschränkt werden. Eine Übersicht über diese Problematik stellt der Datenschutzbeauftragte auf seiner Website im Leitfaden Auslagerung: Berücksichtigung des CLOUD Act detailliert dar.

Zum Einsatz von Office 365 in der Verwaltung hat der Datenschutzbeauftragte versucht, sich mit Microsoft in datenschutzrechtlichen Belangen auf Schweizer Recht und einen schweizerischen Gerichtsstand zu einigen. Diese Faktoren wären bei Vertragsabschluss einzufordern. Microsoft hat sich nicht auf die vorgeschlagene Formulierung festgelegt.

In seiner Antwort auf die Anfrage eines Amtes zu den Bedingungen für die Ausschreibung einer neuen Arbeitsplatzumgebung schrieb der Datenschutzbeauftragte, dass die Anbieter begründet darzulegen haben, falls sie gewisse datenschutzrechtliche Anforderungen nicht erfüllen können. Das öffentliche Organ kann dann einen Entscheid für oder gegen Cloud Computing fällen, bei dem alle Aspekte berücksichtigt wurden.

Elektronischer Zugriff auf Personaldossiers

Nach Einführung des E-Personaldossiers in der kantonalen Verwaltung können Führungskräfte über ein Portal auf Informationen in den Personaldossiers der Mitarbeitenden elektronisch zugreifen. Der Datenschutzbeauftragte ging Anfragen nach, in denen kritisiert wurde, dass Führungskräfte über das Portal auf zu wenige Hierarchiestufen ihrer Organisation zugreifen können.

Das Personalamt ist für die Webanwendung verantwortlich. Abklärungen des Datenschutzbeauftragten ergaben, dass der Zugriff auf die Personaldossiers auf zwei Arten beschränkt ist. Einerseits werden der Führungskraft nicht alle im Personaldossier enthaltenen Dokumente angezeigt. Die Führungskraft kann etwa Administrativunterlagen wie Adressänderungen nicht einsehen. Auch sensible Angaben, die die oder der Vorgesetzte nicht zur Erfüllung der Aufgaben braucht, werden nicht angezeigt, beispielsweise Unterlagen eines Case Management oder Lohnabrechnungen. Andererseits erhalten Führungskräfte nur ständigen Zugriff auf die Dossiers von Mitarbeitenden, die maximal zwei Hierarchiestufen tiefer stehen. Auf Anfrage kann die HR-Abteilung dem Vorgesetzten weitere Dossiers zeitlich beschränkt elektronisch freischalten oder die Führungskraft kann direkt bei der HR-Abteilung in die Dossiers Einsicht nehmen.

Der Datenschutzbeauftragte kam zum Schluss, dass die Praxis dem Verhältnismässigkeitsprinzip entspricht. Er merkte an, dass alle Zugriffe auf die Dokumente zu protokollieren sind. Dies betrifft besonders die direkte Einsichtnahme der Führungskraft bei der HR-Abteilung. Die technische Protokollierung erfasst in diesem Fall den HR-Zugriff auf das E-Dossier. Der Zugriff durch die Führungskraft muss zusätzlich protokolliert werden.

Datenspuren für Private

Parkieren im digitalen Zeitalter

Gemeinden und Städte beginnen, die Parkplatzbewirtschaftung umzurüsten. Der freie Parkplatz kann zukünftig digital gesucht und die Gebühr digital bezahlt werden. Die Abrechnung erfolgt auf die Minute genau. Daraus ergibt sich jedoch, dass mehr Informationen erhoben und bearbeitet werden als bisher. Vor der Einführung des digitalen Parkierens ist abzuklären, wer diese zusätzlichen Daten wie und zu welchen Zwecken bearbeitet oder bearbeiten darf.

Zusätzliche Datenbearbeitungen

Bei der Parkplatzbewirtschaftung mit Parkuhren und Münzbezahlung werden Personendaten erst erhoben, wenn eine Kontrolleurin oder ein Kontrolleur feststellt, dass die Gebühr nicht korrekt bezahlt wurde, und ein Bussenverfahren eingeleitet wird. Bei der digitalen Parkplatzbewirtschaftung gehören zu den erhobenen Daten etwa das Autokennzeichen, die genaue Zeit des Parkierens und des Wegfahrens sowie die Standortdaten. Meist werden von den App-Betreibern schon bei der Erstellung eines Nutzerkontos weitere persönliche Daten erhoben. Grundsätzlich ist eine Identifikation der Automobilistin respektive des Automobilisten erst bei Verletzung der Parkvorschriften notwendig.

Bedenken der Bevölkerung

Beim Datenschutzbeauftragten haben sich viele Bürgerinnen und Bürger gemeldet, die besorgt sind über die Einführung der digitalen Parkplatzbewirtschaftung. Sie stellten fest, dass durch die Umstellung von Parkuhren mit Münzeinwurf auf die digitale Bewirtschaftung mehr Daten als bisher erfasst werden, und sind verunsichert, wie diese Daten verwendet werden.

Der Datenschutzbeauftragte wurde gebeten, die Prozesse zu prüfen und die datenschutzrelevanten Aspekte zu beurteilen. In drei Fällen haben sich auch Behörden vor einer solchen Umstellung auf digitales Bezahlen der Parkgebühren an den Datenschutzbeauftragten gewandt, damit er die Rechtmässigkeit überprüfen und die Rahmenbedingungen festlegen kann.

Heute bereits Tatsache

Die digitale Parkplatzbewirtschaftung wurde in der Schweiz an zahlreichen Orten bereits umgesetzt. Anbieter der digitalen Lösungen publizieren, dass sie in 400 Gemeinden und Städten aktiv sind, so auch im Kanton Zürich.

Vor- und Nachteile

Für die Automobilistin und den Automobilisten ergeben sich aus der digitalen Parkplatzbewirtschaftung Vorteile, wie das Finden eines freien Parkplatzes per App, die damit zusammenhängende geringere Suchzeit und das Wegfallen der Münzsuche. Die Behörden rechnen sich vor allem finanzielle und personelle Einsparungen aus, indem etwa die Kosten für den Betrieb, den Unterhalt und die Kontrolle der Parkuhren wegfallen. Dem steht entgegen, dass mehr Datenspuren hinterlassen werden, die betroffenen Personen weniger Kontrolle über die eigenen Daten haben und die Datenbearbeitungsprozesse nicht mehr transparent sind. Aus datenschutzrechtlicher Sicht ist zu berücksichtigen, dass bei der digitalen Parkplatzbewirtschaftung verschiedene Organisationen beteiligt sind. Die Verantwortlichkeiten für die Datenbearbeitungen sind unklar. Die erhobenen Daten lassen Auswertungen und Verknüpfungen zu.

Verschiedene Modelle

Die Gemeinden und Städte setzen unterschiedliche Modelle um. In einem Schweizer Kanton wurde eine eigene App entwickelt. Die weiteren Modelle reichen bis hin zur kompletten Auslagerung der Parkplatzbewirtschaftung. Für die Beurteilung der Lösungen sind die verschiedenen Prozessschritte zu unterscheiden. Es sind dies

- die Parkplatzbewirtschaftung selbst, bei welcher die Nutzung des öffentlichen und allenfalls privaten Grundes überprüft wird,
- der Zahlungsvorgang,
- der Kontrollvorgang, ob die Parkzeit überschritten wurde,
- das Bussenverfahren, falls die Parkzeit überschritten wurde.

Bei der erwähnten kantonseigenen App bleiben die erhobenen Daten unter der Kontrolle der öffentlichen Verwaltung. Die Verantwortlichkeiten sind klar definiert und die Datenflüsse transparent. In diesem Fall werden nur die Daten erhoben, die zur Überprüfung der Zahlung notwendig sind. Die Automobilistin respektive der Automobilist wird erst identifiziert, wenn ein Bussenverfahren eingeleitet wird. Bei allen anderen Modellen verfügen Dritte über die erhobenen Daten. Wird nur die Parkraumbewirtschaftung an eine externe Firma ausgelagert, so ist auch bei diesem Modell eine datenschutzfreundliche Lösung mit wenig Aufwand umsetzbar. Die Identifikation erfolgt erst mit Einleitung des Bussenverfahrens.

Komplexer wird der Sachverhalt, wenn die Parkplatzbewirtschaftung und der Zahlungsverkehr ausgelagert und miteinander verknüpft werden. Je nach gewählter Art des Zahlungsvorgangs verfügt der Anbieter der Lösung über umfangreiche Daten.

Klare Rahmenbedingungen nötig

Der grössere Umfang der erhobenen Daten und die Tatsache, dass bei den meisten Lösungen Dritte beteiligt sind, erhöhen das Risiko für Eingriffe in die Persönlichkeitsrechte. Ausserdem können die Daten ausgewertet werden. Verknüpfungen von Daten über eine gewisse Zeit hinweg können zu Persönlichkeitsprofilen führen und Überwachungen wären möglich. Mit klaren Rahmenbedingungen können diese Risiken minimiert werden. Fragen zum Rechtsverhältnis zwischen dem öffentlichen Organ und dem Anbieter der Apps sowie dem Betreiber der Datenbanken sind zu klären. Weiter ist zu klären, ob eine ausschliesslich digitale Parkplatzbewirtschaftung erlaubt ist oder ob weiterhin Parkautomaten mit Münzeinwurf zur Verfügung stehen müssen. Zudem muss definiert werden, wie lange die Daten aufbewahrt werden dürfen. Der Datenschutzbeauftragte arbeitet an der Definition der Rahmenbedingungen.

Staatlicher Zugriff auf kommerzielle Bonitätsdatenbanken

Wie jeder Gläubiger interessiert sich auch der Staat für die Bonität seiner Schuldnerinnen und Schuldner. Die Durchsetzung von Forderungen kann sehr aufwendig sein. Deshalb will der Gläubiger vor Einleitung eines Verfahrens die Solvenz einer Schuldnerin oder eines Schuldners prüfen. Kommerzielle Anbieter stellen für solche Überprüfungen Bonitätsdatenbanken zur Verfügung. Als private Unternehmen unterstehen sie der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. Die Nutzung dieser Datenbanken durch öffentliche Organe im Kanton Zürich fällt unter die Aufsicht des Datenschutzbeauftragten des Kantons Zürich.

Die behördliche Nutzung einer kommerziellen Bonitätsdatenbank ist grundsätzlich zulässig. Wenn eine Bonitätsdatenbank gewisse rechtliche Rahmenbedingungen einhält, darf sie durch ein öffentliches Organ konsultiert werden.

Der Datenbankbetreiber erfährt jedoch mit jeder Abfrage durch ein öffentliches Organ, dass sich der Staat für die Bonität einer Person interessiert. Dies ist eine Datenbekanntgabe gemäss IDG. Der Umgang mit dieser Information durch den Datenbankbetreiber muss datenschutzkonform geregelt sein.

Im geprüften Fall enthielt der Vertrag keine Bestimmungen zu den organisatorischen und technischen Massnahmen zum Schutz der übermittelten Personendaten. Weder die Aufbewahrungsdauer war geregelt, noch bestand eine Beschränkung der Zugriffsmöglichkeiten auf bestimmte Personen. Die Daten wären zudem unverschlüsselt übermittelt worden. Der Datenschutzbeauftragte riet von der Nutzung der Datenbank ab.

Daten im Auge behalten

Den Schutz ausgelagerter Daten verbessern

Der Schwerpunkt der Datenschutzreviews lag 2019 auf der Kontrolle von grösseren IT-Dienstleistern, die für Gemeinden, Spitäler und andere öffentliche Organe das Outsourcing des IT-Betriebs erbringen oder als Webprovider tätig sind.

Die aktuellen Bedrohungsszenarien und die zunehmend anspruchsvollere Technik erfordern einen IT-Betrieb auf hohem Sicherheitsniveau mit einer angemessenen Professionalisierung. Bei den Gemeinden ist deshalb eine Tendenz zur Auslagerung des IT-Betriebs festzustellen. Mit den Kontrollen von Auftragnehmern prüft der Datenschutzbeauftragte die Dienstleistungen dort, wo sie tatsächlich erbracht werden. Zudem erzielt er einen Skaleneffekt, weil das Prüfresultat auf alle angeschlossenen Dienstleistungsbezüger angewendet werden kann. Allfällige Verbesserungsmassnahmen entfalten so einen breiten Nutzen.

Bei den Dienstleistern wurde in der Regel eine professionelle Umgebung angetroffen, welche die hohen Anforderungen in den meisten Fällen erfüllen konnte. In einigen Fällen entsprachen die vertraglichen Regelungen nicht den kantonalen Vorgaben, die in den Allgemeinen Geschäftsbedingungen bei der Auslagerung von Informatikleistungen beinhaltet sind. Oft bestanden keine Service Level Agreements mit den Kunden, welche die zu erbringenden Dienstleistungen ausreichend genau und nachvollziehbar beschrieben.

Gemeinden tragen die Verantwortung

In den meisten Fällen fehlten den Gemeinden die Möglichkeiten, um die erbrachten Leistungen zu kontrollieren. Viele Gemeinden waren ungenügend informiert über die Umstände, wie ihr IT-Betrieb erbracht wird. Der Datenschutzbeauftragte rief in Erinnerung, dass auch bei einer Auslagerung das öffentliche Organ die Verantwortung für die Daten und ihre Sicherheit behält.

Der Datenschutzbeauftragte unterstützte Gemeinden und andere kleinere Organe während der Datenschutzreviews und danach bei der Umsetzung von Massnahmen. Er beurteilte Lösungsvorschläge, Konzepte oder Verträge und unterstützte damit die jeweiligen Verantwortlichen auf ihrem Weg zu mehr Informationssicherheit.

Im Zuge unserer Prüfungen und deren Nachkontrollen zeigte sich, dass bei Gemeinden ein grosser Bedarf für Beratungen durch den Datenschutzbeauftragten vorhanden ist. Massnahmen in Bezug auf Datenschutz und Informationssicherheit werden aufgrund von fehlendem IT-Know-how nicht angegangen.

Mängel bei zentralen Plattformen

Der Datenschutzbeauftragte kontrollierte auch zentrale IT-Plattformen der Kantonsverwaltung. Sie bergen ein hohes Risiko für Datenverluste. Zudem kommt ihnen durch ihre Eigenschaft als Datendrehscheibe oder Datenspeicher eine hohe Bedeutung in Sachen Verfügbarkeit zu. Die festgestellten Mängel in der Dokumentation sowie in Verwaltungs- und Kontrollprozessen sind angesichts des hohen Risikos nicht tragbar.

Mehr Informationssicherheit bei weniger Aufwand

Der Datenschutzbeauftragte arbeitete bei den Kontrollen der Gemeinden 2019 erstmals mit der Internen Revision des kantonalen Steueramts zusammen. Sie führt jedes Jahr bei einer hohen Zahl von Gemeinden Steuerprüfungen durch, die auch einzelne Aspekte der Informationssicherheit enthielten.

Um bei Gemeinden doppelte Prüfungen innerhalb kurzer Zeit zu verhindern, werden die Prüfungsplanungen der beiden Stellen neu aufeinander abgestimmt. Der Datenschutzbeauftragte erstellte ein speziell zugeschnittenes Prüfprogramm für die Mitarbeitenden der Steuerrevision und schulte sie, damit sie ihren Prüfauftrag im Bereich Informationssicherheit noch wirksamer ausführen können.

Dank der Zusammenarbeit können mehr Gemeinden kontrolliert und damit das Informationssicherheitsniveau erhöht werden, andererseits werden die Effizienz gesteigert und Synergien genutzt. Zudem werden die Anforderungen an die Gemeinden vereinheitlicht. Die Kontrollen der Internen Revision des Steueramts zeigten in vielen Fällen Verbesserungspotenzial, beispielsweise bei der Regelung der Zugriffs- und Zutrittsrechte.

Unterstützung der Gemeinden

Die Erfahrungen der letzten Jahre zeigten die Schwierigkeiten von Gemeinden, Massnahmen zur Stärkung des Datenschutzes und der Informationssicherheit umzusetzen. Es fehlt kleineren Gemeinden an Zeit, finanziellen Mitteln und dem nötigen Fachwissen, vor allem wenn konzeptionelle Aufbauarbeiten erforderlich sind. Der Datenschutzbeauftragte entwickelte ein Selbstdeklarationsmodell, das die Gemeinden bei der kontinuierlichen Verbesserung ihrer Informatik- und Kommunikationsstrukturen unterstützt.

Für das Selbstdeklarationsmodell stellt der Datenschutzbeauftragte ein Set von Vorgaben und Vorlagen zusammen, das die Mindestanforderungen im Hinblick auf Datenschutz und Informationssicherheit beschreibt und dabei Faktoren wie Grösse der Gemeinde, Anzahl der Mitarbeitenden, IT-Betriebsmodell und eingesetzte Technologien berücksichtigt. Die Dokumente sind so gestaltet, dass die Gemeinden die Massnahmen umsetzen können, ohne über vertiefte Kenntnisse verfügen oder zeitraubende konzeptionelle Arbeiten erbringen zu müssen.

Zu Beginn der Kontrolle nach dem neuen Modell wird die Gemeinde zum Vorgehen und zu den umzusetzenden Massnahmen beraten. In der nächsten Phase setzt die Gemeinde die vorgeschlagenen Massnahmen um. Der Datenschutzbeauftragte kontrolliert danach die Umsetzung und stellt eine Bestätigung aus, wenn die Gemeinde alle Vorgaben erfüllt. Das Selbstdeklarationsmodell baut darauf auf, dass die Gemeinde sich verpflichtet, die Massnahmen auch nach der Kontrolle periodisch zu prüfen und zu aktualisieren. Es wurde an der Versammlung der IG ICT der Gemeinden vorgestellt und stiess auf breite Zustimmung.

Umfrage und Kontrolle bei der KESB

Die Kindes- und Erwachsenenschutzbehörden (KESB) bearbeiten höchst sensitive Personendaten wie medizinische und psychiatrische Gutachten, Details aus dem familiären Umfeld, finanzielle Daten oder polizeiliche Akten.

Der Datenschutzbeauftragte hat im Jahr 2019 bei allen KESB eine Umfrage durchgeführt, um Informationen zu ihrer Grösse, Organisation und ihrem IT-Betrieb zu sammeln. Aufgrund dieser Angaben erfolgte eine Auswahl der KESB, deren IT-Betrieb nicht an eine Gemeinde oder Stadt angeschlossen ist. Der Datenschutzbeauftragte beginnt 2020 mit einer Kontrollreihe bei verschiedenen KESB, um sicherzustellen, dass die Massnahmen zum Datenschutz und zur Informationssicherheit der Bearbeitung der höchst vertraulichen Daten angemessen sind.

ISMS für die kantonale Verwaltung

Am 1. Januar 2020 trat die Verordnung über die Informationsverwaltung und -sicherheit (IVSV) in Kraft. Zusätzlich wurde eine Allgemeine Informationssicherheitsrichtlinie eingeführt, die durch Besondere Richtlinien und Basiskonfigurationen die Vorgaben detailliert regeln sollen. Mit der IVSV soll der Kanton Zürich ein modernes Informationssicherheits-Managementsystem (ISMS) und einheitliche Vorgaben für alle öffentlichen Organe des Kantons erhalten.

Der Datenschutzbeauftragte war in die Vernehmlassungen involviert, wurde jedoch nicht in die Erstellung miteinbezogen. Die Beanstandungen an den eingereichten Dokumenten waren deshalb entsprechend umfangreich.

Für die Erstellung der besonderen Richtlinien kam nun mit dem Amt für Informatik (AFI) eine Zusammenarbeit zustande, wodurch Informationssicherheitsspezialisten des Datenschutzbeauftragten bei der Ausarbeitung der Richtlinien mitarbeiten können. Der Datenschutzbeauftragte begrüsst die Möglichkeit, sich frühzeitig einbringen zu können. Somit fliesst neben seinem spezifischen Fachwissen auch die Erfahrung aus seiner umfassenden Kontrolltätigkeit in die Richtlinien ein.

Entschlüsselung von sicheren Verbindungen

Die Verschlüsselung der Webverbindungen mit dem https-Protokoll ist eine wesentliche Massnahme zum Schutz der Privatsphäre im Internet. Allerdings verwenden Malware-Websites verschlüsselte Verbindungen, um der Entdeckung durch Malwarescanner und ähnliche Systeme zu entgehen. Damit die öffentlichen Organe und ihre IT-Dienstleister gegen solche Angriffe gewappnet sind und Malware herausgefiltert werden kann, werden die Verschlüsselungen oft aufgebrochen. Die Entschlüsselung greift in die Privatsphäre der betroffenen Personen ein, tangiert aber auch die Integrität und Authentizität von Online-Transaktionen. Der Datenschutzbeauftragte hat in seinen Beratungen und Kontrollen festgestellt, dass die Entschlüsselung von Webverbindungen in den meisten Fällen nicht datenschutzkonform ist.

Die Checkliste Entschlüsselung von Webverbindungen auf der Website des Datenschutzbeauftragten zeigt, welche Voraussetzungen erfüllt sein müssen, damit eine Entschlüsselung erlaubt ist. Die folgenden Massnahmen sind dafür zu beurteilen:

- In einer Risikoanalyse und -beurteilung ist aufzuzeigen, dass die Massnahmen zur Risikominderung das Aufbrechen der Verbindung rechtfertigen.
- Die Nutzerinnen und Nutzer sind transparent über die Entschlüsselung zu informieren.
- Über einen definierten Prozess müssen bestimmte Websites von der Entschlüsselung ausgenommen werden können.
- Die Zertifikate für die verschlüsselten Webverbindungen müssen korrekt umgesetzt und behandelt werden.
- Die nötigen technischen Massnahmen für den Betrieb der Internetsurf-Proxy-Infrastruktur müssen sichergestellt sein.
- Die Anforderungen an die Auslagerung von Datenbearbeitungen sind einzuhalten, falls der Internetsurf-Proxy von einem Auftragnehmer betrieben wird.

Fachexpertise in den Gemeinden

Mit der Digitalisierung werden in der Verwaltung immer mehr Prozesse automatisiert oder mithilfe neuer Technologien optimiert. Das Resultat ist ein ständig wachsender Datenfluss. Oft ist es für Verantwortliche in Digitalisierungsprojekten schwierig, die rechtliche und technische Tragweite ihrer Entscheidungen abzuschätzen. Wie können die Informationssicherheit und der Datenschutz praktisch umgesetzt werden? Wie können die betroffenen Mitarbeitenden einbezogen werden? Mit diesen und anderen praxisorientierten Fragen beschäftigten sich 15 Teilnehmerinnen und Teilnehmer im Seminar Informationssicherheit für Gemeinden.

Zu den Lernzielen des Seminars gehörten die datenschutzrechtlichen Anforderungen an die Bearbeitung von Personendaten. Kleine und grosse Gemeinden haben die gleichen gesetzlichen Voraussetzungen an die Informationssicherheit zu erfüllen. Die Teilnehmenden lernten an praktischen Beispielen, die Vorlagen, Anleitungen und Checklisten des Datenschutzbeauftragten anzuwenden.

Gemeinden haben angemessene technische und organisatorische Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität umzusetzen. So steht es im Gesetz über die Information und den Datenschutz (§ 7, IDG, LS 170.4). Werden Dienstleistungen durch einen Auftraggeber erbracht, sind die Verträge datenschutzkonform zu gestalten. Dazu gehören datenschutzkonforme Allgemeine Geschäftsbedingungen (AGB). Das Amt für Informatik (AFI) stellt auf seiner Website die AGB Auslagerung Informatikleistungen und die AGB Datenbearbeitung durch Dritte zur Verfügung.

Die Komplexität und Heftigkeit der Angriffe auf die IT-Struktur auch von Gemeinden und anderen öffentlichen Organen verlangt nach einem bewussten und strukturierten Umgang mit den Risiken und technisch-organisatorischen Massnahmen. Die Grundlage dafür bilden eine angemessene Organisation und Ziele zur Sicherstellung der Informationssicherheit. Die Vorlagen auf der Website des Datenschutzbeauftragten helfen bei der Umsetzung der nötigen Massnahmen zur Gewährleistung der Informationssicherheit und des Datenschutzes.

Das alltägliche Verhalten der Mitarbeitenden und der Vorgesetzten bestimmt das Sicherheitsniveau einer Organisation. Deshalb sind alle Beteiligten zu schulen und zu sensibilisieren, damit eine Sicherheitskultur entsteht. Dafür eignen sich Informationen in einem persönlichen Gespräch oder an einer Teamsitzung wie auch ein spezifischer Themenworkshop, beispielsweise zum Thema Sichere Passwörter. Weitere Anregungen und Möglichkeiten enthält die Anleitung Sensibilisierung der Mitarbeitenden für Informationssicherheit auf der Website des Datenschutzbeauftragten.

Bekanntgabe der Adressen von Beiständen an Einwohnerkontrolle

Die Weitergabe von Personendaten durch ein öffentliches Organ an ein anderes öffentliches Organ muss gesetzlich vorgesehen sein. Trotzdem kann unklar erscheinen, welche Informationen von einer vorhandenen Rechtsgrundlage umfasst sind. Ein Amt wandte sich an den Datenschutzbeauftragten und wollte wissen, ob die Einwohnerkontrolle einer Gemeinde von einem Kinder- und Jugendhilfezentrum (KJZ) Informationen über Kindesschutzmassnahmen erwarten darf. Die Einwohnerkontrolle wollte den Namen des Beistands im System erfassen und über Adressänderungen informiert werden. Der Datenschutzbeauftragte wies die Einwohnerkontrolle darauf hin, dass Kindes- und Erwachsenenschutzbehörden der Gemeinde Regelungen betreffend die elterliche Sorge über minderjährige Personen melden. Diese Meldung umfasst Namen und Adressen der sorgeberechtigten Personen. Darunter fallen auch Fälle, in denen die elterliche Sorge nur in gewissen wichtigen Bereichen beschränkt wurde und diese Bereiche einem Beistand übertragen worden sind. Besuchsbeistände sind davon allerdings nicht erfasst.

Herausforderung Gesundheitsdaten

Schutz der Gesundheitsdaten als Herausforderung

Datenschutz findet im Gesundheitsbereich grundsätzlich eine ideale Ausgangslage vor: Fast allen ist der hohe Schutzbedarf von Gesundheitsdaten bewusst. Die komplexe Organisation des Gesundheitswesens mit den vielen unterschiedlich strukturierten Akteuren stellen die Verantwortlichen jedoch vor grosse Herausforderungen. Das datenschutzrechtliche Fachwissen in den Gesundheitseinrichtungen wächst kontinuierlich. Der Dialog des Datenschutzbeauftragten mit den Akteuren im Gesundheitsbereich führt zur konstruktiven und praxisnahen Lösungsfindung.

Der Datenschutzbeauftragte begleitete die Einführung des Elektronischen Patientendossiers im Universitätsspital Zürich. In Bezug auf die Klinikinformationssysteme (KIS) hat der Datenschutzbeauftragte seinen engen Austausch mit den Spitälern fortgeführt. Besonders im Fokus standen die Dauer der Aufbewahrung für Gesundheitsdaten und der Umgang mit den Daten nach Ablauf der Aufbewahrungsfristen. Oft sehen die KIS keine Löschung vor.

Der Datenschutzbeauftragte erhielt zahlreiche Anfragen zu Datenlecks im Gesundheitsbereich. Einen weiteren Schwerpunkt bildeten Beratungen dazu, wie das Einsichtsrecht in Patientendokumentationen wahrgenommen werden kann. Zusätzlich interessieren sich Patientinnen und Patienten dafür, welche Personen im Spitalalltag auf ihre Patientendokumentationen zugreifen können.

Die technologischen Entwicklungen im medizinischen Bereich stellen etablierte Herangehensweisen infrage, auch im Bereich des Datenschutzes. So stellt sich die Grundsatzfrage nach der Anonymisierungsmöglichkeit von genetischen Daten, aber auch von Daten in der personalisierten Medizin.

Im Hinblick auf die künftigen Entwicklungen ist der fachliche Austausch mit den Forschenden wichtig. Der Datenschutzbeauftragte begleitete 2019 mehrere Forschungsprojekte zu unterschiedlichen Themen wie Emotionsanalyse in Tweets, Altersvorsorge, Arbeitsmarktbeobachtung und Durchimpfungsraten. Bei den forschenden Institutionen sind ein hohes Bewusstsein für den Schutz der Privatsphäre sowie datenschutzrechtliches Grundwissen vorhanden. Sie fragten vor allem nach Beratungen zur praktischen Umsetzung der gesetzlichen Anforderungen, gerade auch im Hinblick auf den Einsatz von technischen Mitteln wie Umfrageplattformen und Datenaustauschlösungen.

Die interdisziplinäre Zusammenarbeit der Fachpersonen aus den Bereichen Recht und Informationssicherheit ermöglicht dem Datenschutzbeauftragten die kompetente Beratung im Gesundheitsbereich.

Nie im Spital und trotzdem registriert

Der Datenschutzbeauftragte beriet eine Institution im Gesundheitswesen beim Umgang mit behandlungswilligen Personen, die ihre Meinung über einen Klinikeintritt kurzfristig änderten. Gerade bei psychischen Erkrankungen kann ein stationärer Aufenthalt mit der Angst vor Stigmatisierung verbunden sein. Es kommt daher vor, dass sich Patienten nach erfolgter Überweisung oder Anmeldung doch gegen einen Klinikeintritt entscheiden.

Bei Überweisungen durch vorbehandelnde Ärzte sind in solchen Fällen bereits medizinische Angaben zur Patientin oder zum Patienten vorhanden. Auch bei Selbsteinweisungen können vorgängig telefonische Beratungsgespräche geführt worden sein, die der medizinischen Dokumentationspflicht unterliegen. Patientendokumentationen sind gemäss gesetzlicher Regelung mindestens zehn Jahre aufzubewahren. Eine Person, die sich gegen einen Klinikeintritt entscheidet, mag aber ein Interesse an der Löschung von Einträgen haben, die sie als stigmatisierend empfindet.

Der Datenschutzbeauftragte riet der Institution, bei informellen oder rein administrativen Anfragen zunächst auf eine Erfassung im Klinikinformationssystem (KIS) zu verzichten. Sobald ein medizinisches Vorgespräch stattgefunden hat, ist dies im KIS zu dokumentieren. Ebenfalls aufzunehmen sind allfällige Unterlagen, die im Rahmen einer Überweisung übermittelt wurden. Diese Informationen sind gemäss der gesetzlichen Dokumentationspflicht aufzubewahren, selbst wenn die Behandlung vor Klinikeintritt abgebrochen wird.

Die Zusammenarbeit der Aufsichtsinstanzen verlief bei dieser Beratung sehr gut. Der Datenschutzbeauftragte konnte in dieser Sache in enger Absprache mit der Gesundheitsdirektion beraten.

Sicherheitsprüfung des Krebsregisters

Der Datenschutzbeauftragte wurde eingeladen, das Informationssicherheits- und Datenschutzkonzept des Krebsregisters Zürich zu prüfen.

Das Krebsregister entstand bereits 1980. Inzwischen wird es vom Institut für Sozial- und Präventivmedizin betrieben mit einem Leistungsauftrag der Kantone Zürich und Zug. Es ist in die Informatikstruktur des Universitätsspitals Zürich integriert und dem Informationssicherheits-Managementsystem (ISMS) unterstellt. Die Datensammlung für das Krebsregister erfolgte bislang auf freiwilliger Basis durch Ärzte, Pathologen und Spitäler. Die Daten werden personalisiert erhoben.

Ab 1. Januar 2020 sind das Bundesgesetz sowie die Verordnung in Kraft getreten, wodurch die Erfassung von Krebserkrankungen in der ganzen Schweiz und somit auch in den kantonalen Krebsregistern obligatorisch wird. Die Registrierung geschieht auch künftig über das bestehende dezentrale System. Die nationale Krebsregistrierungsstelle führt die Daten anschliessend zusammen und arbeitet sie auf. Ärztinnen und Ärzte müssen ihre Patientinnen und Patienten mündlich und schriftlich über ihre Rechte, den Datenschutz und über Art, Zweck und Umfang der Datenbearbeitung informieren. Patientinnen und Patienten können der Registrierung ihrer Daten jederzeit widersprechen.

Da es sich bei diesen Daten um höchst sensitive Personendaten handelt, berät der Datenschutzbeauftragte das Krebsregister Zürich auch in Zukunft, um die entsprechenden Anforderungen bei der Informationssicherheit und beim Datenschutz sicherzustellen.

Revision des Spital-planungs- und -finan-zierungsgesetzes

Der Datenschutzbeauftragte nahm Stellung im Rahmen der Vernehmlassung zur Revision des Spitalplanungs- und -finanzierungsgesetzes (SPFG). Die Revision beinhaltet die Aufnahme von zusätzlichen qualitativen Anforderungen an die Leistungserbringer. Damit soll der Regierungsrat mit den Leistungsaufträgen verbundene Anforderungen festlegen, beispielsweise zum Qualitätscontrolling. Der Datenschutzbeauftragte hat vorgeschlagen, dass nicht nur Vorgaben zum Qualitätscontrolling, sondern auch zum Datenschutz und zur Informationssicherheit festgehalten werden. Die Gesundheitsdirektion teilt diese Ansicht.

Spitäler sollen über die Spitalliste stärker auf ihre Pflichten zur Wahrung des Datenschutzes und der Informationssicherheit hingewiesen werden und zum Aufbau und zur Pflege von Managementsystemen verpflichtet werden, beispielsweise in Form eines Informationssicherheits-Managementsystems (ISMS). Der Datenschutzbeauftragte hielt als Anforderungskatalog für Datenschutz und Informationssicherheit zur Ergänzung im Spitallistenanhang fest:

- Es ist ein Managementsystem für Datenschutz und Informationssicherheit vorhanden und dokumentiert.
- Die Verantwortungen für Datenschutz und für Informationssicherheit sind geregelt.
- Die Verantwortlichen für Datenschutz und für Informationssicherheit sind für ihre Aufgaben geschult und verfügen über die notwendigen Ressourcen und Kompetenzen.
- Die Verantwortlichen für Datenschutz und für Informationssicherheit sind in die wesentlichen Informations- und Datenbearbeitungsprozesse und in die wesentlichen Projekte einbezogen. Die Art und Weise des Einbezugs ist in den Betriebsprozessen und im Projektmanagement geregelt.
- Die Managementsysteme für Datenschutz und Informationssicherheit werden in einem kontinuierlichen PDCA-Zyklus laufend verbessert (PDCA: Plan, Do, Check, Act).
- Die Schnittstellen und Abgrenzungen von Risikomanagement, Qualitätsmanagement und Compliance zum Datenschutz- und Informationssicherheitsmanagement sind geregelt.

Der Datenschutzbeauftragte erarbeitet einen Vorschlag für einen neuen Abschnitt über den Datenschutz und die Informationssicherheit (Datenschutz-Managementsystem) und die entsprechenden Mindestanforderungen an die Spitäler für den vollständig überarbeiteten Spitallistenanhang «Generelle Anforderungen».

Änderung des DNA-Profil-Gesetzes

Der Datenschutzbeauftragte nahm Stellung zur Änderung des Bundesgesetzes über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (DNA-Profil-Gesetz). Er kam zum Schluss, dass das neu eingeführte Verfahren zur Feststellung äusserlich sichtbarer Merkmale einer Person (Phänotypisierung) und der erweiterte Suchlauf mit Verwandtschaftsbezug (Verwandtenrecherche) hohe Anforderungen an die gesetzliche Grundlage stellen und beurteilte die Vorlage mit einigen Vorbehalten als angemessen.

Bei der Verwandtenrecherche wird in der Datenbank nach Personen gesucht, die mit der Spurgeberin oder dem Spurgeber am Tatort verwandt sein könnten. Sie ist eine Bearbeitung von sensitiven Personendaten und stellt einen starken Eingriff in die Persönlichkeitsrechte dar. Der Datenschutzbeauftragte wies darauf hin, dass keine der bisher durchgeführten Verwandtenrecherchen zu einem Ermittlungserfolg geführt hat. Deshalb beurteilte er sie als nicht ohne weiteres verhältnismässig. Weiter wies er darauf hin, dass besondere Anforderungen zu stellen sind an die Bestimmtheit der gesetzlichen Grundlage für die Bearbeitung sensitiver Personendaten. Der Datenschutzbeauftragte erachtet die Umschreibung des Gesetzeszwecks als zu wenig bestimmt und fordert eine Präzisierung.

Der Datenschutzbeauftragte wies darauf hin, dass auch die Phänotypisierung ein schwerer Eingriff in die Persönlichkeitsrechte der betroffenen Personen darstellt. Er stellte fest, dass nur die subsidiäre Anwendung dieser Massnahme verhältnismässig ist, und forderte, diese ausdrücklich im Gesetz zu regeln.

Der Datenschutzbeauftragte begrüsste, dass die Verwandtenrecherche wie auch die Phänotypisierung ausschliesslich bei Verbrechen angewandt wird. Er forderte jedoch eine Verschärfung dieser Regelung. Beide Massnahmen sollten nur bei schweren Verbrechen eingesetzt werden, für die ein Deliktskatalog zu erstellen ist. Der Datenschutzbeauftragte verlangte, dass beide Massnahmen durch das Zwangsmassnahmengericht angeordnet werden sollen, wie dies bereits heute für Massenuntersuchungen gilt.

Der Mensch ist das Mass

Datenschutz ohne Grenzen

Die Digitalisierung ist eine globale Entwicklung und der Kanton Zürich ist wie die Schweiz als Gesamtes abhängig von internationalen Hardware-, Software- und Dienstleistungsanbietern. Je mehr die Datenbearbeitungen in die Cloud ausgelagert werden, desto mehr ist dies der Fall. Die Datensouveränität und mit ihr der Datenschutz sind in diesem Umfeld besonders wichtig. Um im eigenen Umfeld die richtigen Entscheide zu treffen, ist es wichtig, die internationalen Entwicklungen zu kennen. Dies trifft auf alle Bereiche zu, so auch auf den Datenschutz.

Der Datenschutzbeauftragte verfolgt deshalb die internationalen Entwicklungen und nimmt am Austausch mit anderen Datenschutzbehörden teil, wie er sich im Rahmen der Schengen-Zusammenarbeit der Schweiz mit der EU unter den Datenschutzbehörden etabliert hat oder sich bei europäischen oder internationalen Datenschutzkonferenzen ergibt. Bei der Schengen-Zusammenarbeit fliessen die Resultate zurück an die Konferenz der Kantonsregierungen (KdK) im Rahmen der Begleitorganisation Schengen / Dublin (BOSD).

Konferenzen dienen dem gegenseitigen Austausch zwischen Datenschutzbehörden über konkrete Themenbereiche oder zur Informationsbeschaffung. So entstehen wichtige Kontakte, wenn es beispielsweise darum geht, globale Cloud-Lösungen wie Office 365 datenschutzrechtlich beurteilen zu können und die Voraussetzungen für deren Nutzung im Kanton Zürich zu schaffen (Seite 13).

International rückte die Sensibilisierung von Jugendlichen für den Datenschutz bei den Datenschutzbehörden zunehmend in den Mittelpunkt. In diesem Umfeld wurde auch das Projekt «Geheimnisse sind erlaubt» des Datenschutzbeauftragten zur Kenntnis genommen, das er zusammen mit der Pädagogischen Hochschule (PHZH) entwickelte (TB 2018, Seite 13): Das Lehrmittel für Schulkinder im Zyklus 1 des Lehrplans 21 ist seit Herbst 2019 in der Lehrpersonen-Ausbildung integriert. Es ist online frei verfügbar. Die Internationale Konferenz der Datenschutzbeauftragten hat «Geheimnisse sind erlaubt» im Oktober 2019 mit dem Global Privacy and Data Protection Award ausgezeichnet, was die hohe Qualität des Lehrmittels unterstreicht und auch eine grosse Anerkennung für den Datenschutzbeauftragten bedeutet (Seite 8). Im Newsletter der Global Privacy Assembly wurden unsere Behörde und Projekte im Bereich der Sensibilisierung vorgestellt.

Das Lehrmittel hat auch auf nationaler Ebene grosse Beachtung gefunden. Der Datenschutzbeauftragte hat es zusammen mit der PHZH am 4. Nationalen Fachforum Jugend und Medien und an der Impulstagung 2019 des Schulnetz21 vorgestellt. Die PHZH konnte eine Finanzierung finden, so dass das Lehrmittel in Zusammenarbeit mit Pädagogischen Hochschulen in der französischen, italienischen und rätoromanischen Schweiz in die Landessprachen sowie ins Englische übersetzt werden kann.

Verantwortung für Informationssicherheit übernehmen

Handy Boxenstop – bei dieser Sensibilisierungsinitiative des Datenschutzbeauftragten für die Mitarbeitenden der kantonalen Verwaltung, der Gemeinden und anderen öffentlichen Organen steht die aktive Beteiligung der Interessentinnen und Interessenten im Vordergrund. Die Nachhaltigkeit der Aktion wird gefördert durch die direkte Umsetzung von Sicherheitsratschlägen, die sich nach den konkreten Bedürfnissen der Ratsuchenden richten. Der Slogan ist Konzept: Mehr Sicherheit, mehr Privatsphäre, selbstgemacht.

Im Jahr 2019 konnten bereits über 60 Veranstaltungen durchgeführt werden, bei denen mehr als 1200 Mitarbeitende des Kantons und der Gemeinden individuell beraten wurden. Aufgrund des Erfolgs wurde die Aktion um ein Jahr verlängert. Für das Jahr 2020 sind bereits 40 weitere Termine geplant.

Smartphones gehören zum Alltag. Sie sind mehr als einfache Kommunikationsmittel. Auf ihnen sammeln sich immer mehr Daten an und geschäftliche Informationen vermischen sich mit privaten, etwa wenn die Mailkonten synchronisiert oder Arbeitsprojekte über ein Chatprogramm diskutiert werden. Smartphones werden für Bankgeschäfte, die Navigation oder zum Fotografieren benutzt. Sie enthalten das gesamte Adressbuch und den Kalender mit privaten und geschäftlichen Terminen und dienen der Information oder Unterhaltung durch Musik, Video oder Spiele. Mit dem Smartphone wird das Smart Home gesteuert. Es wird benutzt zum Abschliessen des Autos, zum Freischalten des E-Trottinetts, zum Bezahlen im Supermarkt oder zur Identifikation.

Offene Schnittstellen, drahtlose Kommunikation und Berechtigungen für alle möglichen Applikationen machen die Geräte angreifbar. Schon einfache Schutzmassnahmen helfen, um die grössten Risiken zu minimieren. Der Schutz durch ein Passwort oder einen Fingerabdruck sollte auf keinem Gerät mehr fehlen. Bei Apps sollte immer wieder geprüft werden, welche Berechtigungen warum freigegeben sind.

Mit dem Handy Boxenstopp fördert der Datenschutzbeauftragte das Bewusstsein für Fragen der Privatsphäre und der Informationssicherheit und trägt zur Stärkung der Sicherheitskultur in den öffentlichen Organen bei. Die Einsätze finden in den Ämtern, Gemeinden, Spitälern und anderen öffentlichen Organen statt. Sie werden durch Studierende ausgeführt, die der Datenschutzbeauftragte für dieses Projekt spezifisch geschult hat. Das Feedback auf die Einsätze ist ausgesprochen positiv.

Sicherheitstipps sind im Smartphone-Lexikon auf der datenschutz.ch-App verfügbar.

Der Mensch ist das Mass

Oft wird die Digitalisierung als eine unkontrollierbare Entwicklung dargestellt, der sich Mensch und Staat unterordnen müssen, um den Anschluss nicht zu verlieren. Der Datenschutzbeauftragte weist in seinen Informationsaktivitäten sowie in Aus- und Weiterbildungen darauf hin, dass die Technologieentwicklung nur einen Teil der Digitalisierung ausmacht. Der Mensch bestimmt, wie er die Möglichkeiten nutzen kann und will. Er stellt die Rahmenbedingungen auf. Seine Fähigkeiten bestimmen auch gleichzeitig über die Sicherheit der neuen Systeme.

Herausforderungen diskutieren

Der Datenschutzbeauftragte zeigte 2019 vier Filme, die sich mit unterschiedlichen Aspekten der aktuellen technologischen Entwicklung auseinandersetzen. In den anschliessenden Gesprächen diskutierten Gäste aus Wissenschaft, Verwaltung und Zivilgesellschaft über die Möglichkeiten einer demokratischen Digitalisierung. In den gutbesuchten Veranstaltungen wurde darüber gesprochen, ob wir unsere Kinder in der digitalen Welt einer totalen Überwachung ausliefern und wie dies verhindert werden kann. Besprochen wurden die Risiken der Rekrutierung für extremistische Bewegungen in den sozialen Medien ebenso wie die neue Qualität, die «Cyber» zum altbekannten Phänomen des Mobbings zufügt. Früher war das Mobbing an einen Ort gebunden. Heute verfolgt es die Opfer über das Smartphone 24 Stunden am Tag und in die privatesten Bereiche des Lebens. Weitere Veranstaltungen nahmen die Frage auf nach der Rolle des Menschen in einer Welt mit immer mehr künstlicher Intelligenz, Cyborgs und Robotern. Kann künstliche Intelligenz eine Veranlagung für moralisches Verhalten erhalten oder werden Werte wie Aufrichtigkeit und Vertrauen abgeschafft?

Unbehagen über fehlendes Recht auf Vergessen

Im Internet wird jeder unserer Schritte für immer aufgezeichnet und die Auswertung unserer Aktivitäten bestimmt, wie wir beurteilt werden und was wir zu sehen bekommen. Im vierten Durchgang des Datenschutz-Video-Wettbewerbs unter dem Titel «Das Internet vergisst nie» konnten wieder interessante Beiträge von Youtuberinnen, Youtubern und anderen Videoschaffenden ausgezeichnet werden. Sie zeigen ein Unbehagen über das fehlende Recht auf Vergessen auf digitalen Plattformen. Der Gewinnerbeitrag endet mit der Aussage: Auch wenn du vergessen hast, das Internet vergisst nie.

Digitalisierung verlangt Datenschutzfitness

Die Digitalisierung bietet praktisch unendliche neue Möglichkeiten. Die Anforderungen an die Datenbearbeitungen durch öffentliche Organe richten sich nach den Grundrechten, wie sie in der Bundesverfassung festgelegt sind. Von den Mitarbeitenden öffentlicher Organe wird zunehmende Kompetenz in Datenschutz und Informationssicherheit verlangt. Der Datenschutzbeauftragte führte auch 2019 Aus- und Weiterbildungen durch. Die Zusammenarbeit mit der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) im Zürcher Zentrum für Informationstechnologien und Datenschutz (ITPZ) wurde weitergeführt.

Neben dem CAS Datenschutzverantwortliche fanden am ITPZ Seminare zu Datenschutz und Öffentlichkeitsprinzip, Datenschutz im Sozialbereich sowie zu Informationssicherheit für Gemeinden statt. Der Datenschutzbeauftragte war ebenfalls mit einem Modul innerhalb des CAS Sozialhilferecht der ZHAW beteiligt.

An der Universität Zürich (UZH) bekamen Fachpersonen aus Medizin und Recht im CAS MedLaw die Grundlagen des Datenschutzes vermittelt. Zum CAS Clinical Trial Management der UZH trug der Datenschutzbeauftragte das Modul Datenschutz in der medizinischen Forschung bei.

Im Rahmen der Weiterbildungsprogramme der Pädagogischen Hochschule (PHZH) bearbeitete der Datenschutzbeauftragte mit den teilnehmenden Lehrpersonen und Schulleitenden mögliche datenschutzrechtliche Herausforderungen im Alltag von Mittel- und Berufsschulen. Lernende im kaufmännischen Bereich erhielten vom Datenschutzbeauftragten eine Einführung in das Öffentlichkeitsprinzip, den Datenschutz und das Amtsgeheimnis.

Einbürgerung an der Gemeindeversammlung

Einbürgerungsentscheide an der Gemeindeversammlung stehen im Spannungsgeld zwischen direktdemokratischer Tradition und rechtsstaatlichen Garantien. Die Privatsphäre der einbürgerungswilligen Person wird dabei immer wieder zum Thema. Der Datenschutzbeauftragte verlangte 2017 im Rahmen der Totalrevision der kantonalen Bürgerrechtsverordnung, dass im kantonalen Recht zu regeln sei, welche Informationen den Stimmbürgern zur Meinungsbildung zur Verfügung gestellt werden. Die Forderung blieb unberücksichtigt. 2019 äusserte sich der Datenschutzbeauftragte im Rahmen der Vernehmlassung zur Totalrevision des kantonalen Bürgerrechtsgesetzes erneut dazu.

Während des Einbürgerungsprozesses muss die betroffene Person viel von sich preisgeben. Damit die Stimmberechtigten einen Entscheid treffen können, muss die Gemeinde vor der Gemeindeversammlung Informationen über die einbürgerungswillige Person auflegen. Es wäre unverhältnismässig, den gesamten Bericht über die Einbürgerungsvoraussetzungen für die Stimmbürger offenzulegen. Der Datenschutzbeauftragte fordert, dass im Gesetz mindestens definiert wird, wie mit dem Bericht umzugehen ist. Der Datenschutzbeauftragte schlägt im Rahmen der Vernehmlassung vor, dass den Stimmbürgern eine Zusammenfassung des Berichts zur Verfügung gestellt wird. Mit dieser Konkretisierung im Gesetzeswortlaut soll die Abwägung zwischen Demokratie und Privatsphäre verbindlich, rechtssicher und praxisnah festgelegt werden.

Das Ergebnis der Vernehmlassung und die weiteren Schritte des Regierungsrats sind noch nicht bekannt.

Digital zusammenarbeiten

Digital zusammen-arbeiten

Der Datenschutzbeauftragte konnte die Zusammenarbeit im Bereich der Digitalisierungsprojekte weiter ausbauen, über neue Datenschutzinstrumente sowie deren Umsetzung informieren und gleichzeitig die Integration dieser neuen Instrumente in die Projektmethodik Hermes bewirken.

Aufbau der Zusammenarbeit

Der Datenschutzbeauftragte nahm nach der Verabschiedung der Digitalisierungsstrategie die direkte Zusammenarbeit auf mit den involvierten Stellen der kantonalen Digitalisierungsprojekte. 2019 wurden diese Zusammenarbeiten intensiviert. Mit der Abteilung Digitale Verwaltung und E-Government der Staatskanzlei, die für die Koordination der Projekte des Impulsprogrammes zuständig ist, etablierte sich ein regelmässiger Austausch. In diesen Gesprächen konnte die rechtzeitige Integration des Datenschutzbeauftragten in Digitalisierungsvorhaben thematisiert werden. Die sehr gute Zusammenarbeit machte es dem Datenschutzbeauftragten verschiedene Male möglich, über seine Dienstleistungen und die anstehenden Neuerungen im Datenschutzrecht zu informieren. Seine Informationen stiessen auf grosses Interesse, und er wurde von zahlreichen Projektleiterinnen und Projektleitern für eine Beratung oder Begleitung ihres Projekts angefragt. An einer Mittagsveranstaltung zum Impulsprogramm informierte der Datenschutzbeauftragte über die neuen Datenschutzinstrumente, die im revidierten Gesetz über die Information und den Datenschutz festgehalten sind.

Dank der neu aufgebauten Zusammenarbeiten wurde der Datenschutzbeauftragte zur Beratung und Begleitung zahlreicher Projekte des Impulsprogramms Digitale Verwaltung eingeladen. Er berät das Projektteam beispielsweise in folgenden Projekten: Rechtliche Grundlagen elektronischer Rechtsverkehr DigiLex (IP 2.1), Studie Blockchain (IP 1.5), Strategie Datenmanagement und Data Governance (IP 3.1), Geschäftsarchitektur Digitale Verwaltung und E-Government (IP 7.3), ZHweb2019 (IP 4.1), Erneuerung Transaktionsplattform ZHServices, eBaugesucheZH (IP 1.1), eEinbürgerungenZH (IP 1.2), Online-Bewilligungen (IP 1.4) und Serviceorganisation eFormulare (IP 2.2).

Integration der neuen Datenschutz-Instrumente

Mit der Revision sind im Gesetz über die Information und den Datenschutz (IDG) neue Datenschutzinstrumente verankert worden. Eines dieser Instrumente ist die Datenschutzfolgenabschätzung (DSFA) (§ 10 Abs. 1 IDG). Darin bewerten öffentliche Organe bei einer geplanten Bearbeitung von Personendaten die Risiken für die Grundrechte der betroffenen Personen. Sie dient dem öffentlichen Organ zur Sicherstellung und zum Nachweis der Einhaltung der Datenschutzvorschriften. Die DSFA wird vom öffentlichen Organ selbst vor jeder geplanten Bearbeitung von Personendaten durchgeführt. Stellt das öffentliche Organ dabei besondere Risiken für die Grundrechte der betroffenen Personen fest, hat es das Projekt dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Der Datenschutzbeauftragte schlug vor, dass die DSFA sowie die Vorabkontrolle in der Projektmethode Hermes abgebildet werden. Hermes wurde vom Regierungsrat als Projektmethode für alle Projekte des Impulsprogramms Digitale Verwaltung festgelegt. Die Integration der neuen Datenschutzinstrumente im vorgeschriebenen Projekttool erleichtert die Arbeit der Projektleiterinnen und Projektleiter. Sie werden beim Abarbeiten der Hermes-Checkliste zum richtigen Zeitpunkt auf die Notwendigkeit einer DSFA und die Abklärung für eine Vorabkontrolle aufmerksam gemacht. Die Datenschutzfolgenabschätzung wird in der Hermes-Projektmethode zunächst in der Initialisierungsphase durchgeführt. Bei Veränderungen am Projekt ist die DSFA später erneut durchzuführen. Die Frage nach der Vorabkontrolle wird in Hermes in der Konzeptphase gestellt.

Projektleiterinnen und Projektleiter finden auf der Website des Datenschutzbeauftragten alle weiteren Informationen und Unterlagen für die Durchführung der Datenschutzfolgenabschätzung und der Vorabkontrolle. Er steht den Projektteams in jeder Projektphase für eine Beratung zur Verfügung. Diese Hilfestellung wurde im Rahmen des Impulsprogramms im Jahr 2019 rege genutzt.

Neue datenschutzrechtliche Leitplanken

Der Kantonsrat hat das revidierte Gesetz über die Information und den Datenschutz (IDG) verabschiedet und der Regierungsrat hat eine neue Verordnung zur Informationsverwaltung und -sicherheit (IVSV) erlassen. Während das IDG klare Rahmenbedingungen setzt, verpasst es die IVSV, einheitliche Sicherheitsstandards im Kanton vorzugeben.

Das revidierte IDG setzt die neuen datenschutzrechtlichen Anforderungen um, die sich aus der Schengen-Zusammenarbeit der Schweiz mit der EU und aus der angepassten Konvention 108+ des Europarats ergeben. Eine weitergehende Reform des IDG auf dem Hintergrund der Digitalisierung der Verwaltung hat der Regierungsrat für die Legislatur 2019 – 2023 vorgesehen. Anträge im Kantonsrat, die bereits heute weitere Anpassungen des IDG verlangten, wurden vom Regierungsrat für die neue Reform entgegengenommen.

Das revidierte IDG enthält einige wichtige Bestimmungen, die einerseits klare Rahmenbedingungen für die öffentlichen Organe setzen und andererseits mehr Transparenz über die Datenbearbeitungen für die Bürgerinnen und Bürger bringen.

Öffentliche Organe haben neue Projekte mit einer Risikoabwägung auf die Folgen für die Persönlichkeitsrechte der Bürgerinnen und Bürger zu prüfen. Vorhaben mit besonderen Risiken sind wie bisher dem Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten. Öffentliche Organe stellen mit Organisationsvorschriften sicher, dass die Datenschutzbestimmungen eingehalten werden. Bei Datenschutzverletzungen hat das öffentliche Organ den Datenschutzbeauftragten beizuziehen.

Der Datenschutzbeauftragte hat neu die Kompetenz, das öffentliche Organ mit einer Verfügung zu einer datenschutzkonformen Bearbeitung zu verpflichten. In einem ersten Schritt gibt er wie bisher eine Empfehlung ab. Er kann aber auch aufgrund des Verwaltungsrechtspflegegesetzes (VRG) vorsorgliche Massnahmen verfügen, wie dies der Regierungsrat in seiner Weisung zum IDG ausführt. Weiter beaufsichtigt der Datenschutzbeauftragte neu auch die öffentlichen Organe, die privatrechtlich handeln, wie die Zürcher Kantonalbank.

Beschwerden von Bürgerinnen und Bürger hat der Datenschutzbeauftragte in jedem Fall zu bearbeiten, wie der Regierungsrat in der Weisung festhält. Damit wird das Instrument der Individualbeschwerde gestärkt.

Mit der IVSV wurde die bisherige Informatiksicherheitsverordnung (ISV) auf Ende 2019 ausser Kraft gesetzt. Die ISV hatte ausführliche Bestimmungen, wie die öffentlichen Organe die Sicherheit ihrer Datenbearbeitungen zu gewährleisten hatten. In zahlreichen Teilen war sie inhaltlich und begrifflich veraltet. Mit der IVSV wurde ein Ersatz geschaffen, der jedoch inhaltlich nicht gleichwertig ist. Es handelt sich um wenige Rahmenbedingungen, die für die Praxis nur hilfreich sind, wenn konkrete Leitplanken geschaffen werden. Das Amt für Informatik (AFI) erstellt diese zurzeit für die kantonale Verwaltung. Wie die Gemeinden, Hochschulen und weiteren öffentlich-rechtlichen Anstalten diese Konkretisierung vornehmen werden, bleibt offen. Angesichts der zunehmenden Digitalisierung und den damit einhergehenden Sicherheitsrisiken, erscheint es aus heutiger Sicht fahrlässig, in diesem Bereich für den Kanton Zürich keine einheitlichen Standards zu setzen.

Datenschutz-erklärungen, Banner, Pop-ups und andere Scheinlösungen

Fast jede Website ist heute mit einer Datenschutzerklärung versehen. Die Nutzerinnen und Nutzer sollen darüber aufgeklärt werden, in welche Datenbearbeitungen sie explizit oder implizit einwilligen. Im privatrechtlichen Bereich ist dies vorgeschrieben. Vor allem im Geltungsbereich der EU-Datenschutz-Grundverordnung (DSGVO) kommen noch die allgegenwärtigen Banner und Pop-ups dazu, die eine ausdrückliche Einwilligung in die Verwendung von Cookies und Auswertungen verlangen. Anlässlich der Neugestaltung des Internetauftritts der kantonalen Verwaltung prüfte der Datenschutzbeauftragte die Rechtslage für Websites öffentlicher Organe vertieft.

Öffentliche Organe brauchen für ihre Datenbearbeitungen eine Rechtsgrundlage. Die Einwilligung der Betroffenen kann diese Grundlage nicht ersetzen. Das gilt auch für den Umgang mit Daten, die bei der Website-Nutzung anfallen. Personenbezogene Auswertungen mit Cookies oder Tracking Tools sind für Websites öffentlicher Organe nicht erlaubt.

Der Datenschutzbeauftragte kommt zum Schluss, dass öffentliche Organe für ihre Websites keine Datenschutzerklärungen erstellen müssen. Gleichzeitig rät der Datenschutzbeauftragte davon ab, Mechanismen wie Cookie-Warnungen einzusetzen, die dem Nutzer eine Einwilligung vorgaukeln. Damit würde ein missverständlicher Eindruck erweckt. Der Betrieb einer datenschutzfreundlichen, gesetzeskonformen Behörden-Website kommt ohne solche Scheinlösungen aus.

Nationales System zur Abfrage von Adressen

Der Vorentwurf für das Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen (Adressdienstgesetz) bildet die Grundlage für die Errichtung eines nationalen Adressdienstes. Verwaltungen und Dritte mit gesetzlichem Auftrag sind in den unterschiedlichsten Geschäftsfällen darauf angewiesen oder rechtlich dazu verpflichtet, Personen schriftlich zu kontaktieren. Dazu benötigen sie die aktuellen Adressen dieser Personen, um Fehlzustellungen zu vermeiden. Die Einwohnerkontrollen der Gemeinden verfügen über aktuelle Adressdaten ihrer Einwohnerinnen und Einwohner. Ein neuer nationaler Adressdienst soll verhindern, dass Behörden bei allen in Frage kommenden Gemeinden Adressabklärungen vornehmen und diese zahlreiche unnötige Anfragen beantworten müssen. Für den nationalen Adressdienst wird auf den bestehenden Datenlieferungsprozessen aufgebaut.

Kantone und Gemeinde erheben gestützt auf das Registerharmonisierungsgesetz heute Adressdaten und übermitteln sie an das Bundesamt für Statistik. Sie werden neu auf Bundesebene in einem Informationssystem zusammengefasst und allen Gemeinwesen in einer einheitlichen Form und über eine einheitliche Schnittstelle zur Verfügung gestellt.

Der Datenschutzbeauftragte prüfte, ob im Vorentwurf die datenschutzrelevanten Punkte ausreichend geregelt sind. Die erhobenen Adressdaten sind Personendaten, jedoch keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile. Der Zugriff auf das Informationssystem ist beschränkt auf Behörden, Organisationen und Personen, die zur Erfüllung ihrer gesetzlichen Aufgaben die Adressen der natürlichen Personen in der Schweiz benötigen und die die AHV-Nummer systematisch verwenden dürfen. Das Auskunftsrecht der betroffenen Personen ist im Vorentwurf ausdrücklich geregelt. Die Zugriffe auf die Daten des Informationssystems werden protokolliert, damit nachvollziehbar ist, wer wann auf sie zugegriffen hat. Die Dauer der Aufbewahrung sowie die Vernichtung der Daten sind geregelt. Die Verantwortung für den Schutz der Daten im nationalen Adressdienst wird dem Bundesamt für Statistik übertragen. Der Erlass von Ausführungsbestimmungen wird an den Bundesrat delegiert. Der Vorentwurf zum Adressdienstgesetz schafft die notwendigen gesetzlichen Grundlagen für diese Delegation.

Der Datenschutzbeauftragte beurteilte den Vorentwurf zum Adressdienstgesetz als datenschutzkonform.

Online-Publikation von Einbürgerungs-daten

Bei der Publikation von Personendaten auf einer Website stellt sich die Frage, welche dieser Personendaten zu welchem Zeitpunkt wieder gelöscht werden müssen. Der Datenschutz-beauftragte beschäftigte sich mit dieser Frage im Zusammen-hang mit Ratsprotokollen eines Gemeindeparlaments, die auf der Website publiziert waren. Die Protokolle enthielten auch Informationen zu Einbürgerungsgeschäften. Anfang 2018 trat eine neue Bestimmung der Kantonalen Bürgerrechtsverordnung in Kraft, wonach Angaben zu Einbürgerungsgeschäften nach Eintritt der Rechtskraft des Einbürgerungsentscheids aus dem Protokoll gelöscht werden müssen.

Eine Gemeinde fragte den Datenschutzbeauftragten, ob diese Bestimmung auch für die Gemeinderatsprotokollen aus dem Zeitraum vor Inkrafttreten der neuen Bestimmung gelte. Die neue Bestimmung sorgt dafür, dass die Informationen zu Einbürgerungsgeschäften gelöscht werden, sobald die Veröffentlichung ihren Zweck erfüllt hat. Der Datenschutz-beauftragte wies darauf hin, dass sich diese Pflicht bei der Publikation von Einbürgerungs-daten im Internet schon aus dem verwaltungs- und datenschutzrechtlichen Grundsatz der Verhältnismässigkeit ergebe, ganz unabhängig von der neuen Bestimmung. Die Publi-kation von Einbürgerungsdaten hat zum Zweck, die Öffentlichkeit über aktuell erfolgte Einbürgerungen zu informieren. Das Informationsinteresse der Öffentlichkeit nimmt in der Zeitachse laufend ab, während das Interesse der betroffenen Personen am Schutz ihrer Privatsphäre zunimmt. Der Datenschutzbeauftragte kam zum Schluss, dass die Informationen zu den Einbürgerungsgeschäften aus den Gemeinderatsprotokollen und anderen Dokumente zu entfernen sind, auch wenn diese vor Inkrafttreten der neuen Bestimmung auf der Website veröffentlicht worden sind.

Unser Leitbild

Wir, der Datenschutzbeauftragte des Kantons Zürich und sein Team, setzen uns für das Menschenrecht auf Privatsphäre ein.

Wir nehmen die Herausforderungen der Digitalisierung an und bringen uns bei neuen Entwicklungen und Trends in Gesellschaft und Politik ein.

Wir engagieren uns dafür, dass das Thema Privatsphäre präsent ist.

Wir arbeiten eng mit den öffentlichen Organen des Kantons Zürich zusammen.

Wir setzen uns aktiv dafür ein, dass der Datenschutz in der Gesetzgebung berücksichtigt wird.

Wir sorgen konsequent dafür, dass die öffentlichen Organe die Gesetze zum Datenschutz einhalten.

Wir erfüllen unseren Auftrag interdisziplinär.

Wir arbeiten gezielt mit nationalen und internationalen Organisationen zusammen.

Kontakt

E-Mail	datenschutz@dsb.zh.ch
Adresse	Datenschutzbeauftragter des Kantons Zürich, Postfach, 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, Dufourstrasse 107, 8008 Zürich
Grafik	TKF Kommunikation & Design, t-k-f.ch

Der Tätigkeitsbericht 2019 ist elektronisch verfügbar unter
www.datenschutz.ch/tb2019.

ISSN 2571-5003

Datenschutz mit Qualität

datenschutz.ch