



Überblick

07 Konsequenter Datenschutz braucht Ressourcen

10 Leistungsindikatoren im KEF

Konsequenter Datenschutz braucht Ressourcen

Im Jahr 2018 hat der Regierungsrat die Strategie «Digitale Verwaltung 2018 – 2023» verabschiedet und mit einem Impulsprogramm zusätzliche finanzielle und personelle Mittel für eine rasche Umsetzung gesprochen. «Konsequent digital» heisst die neue Vorgabe für die Verwaltung. «Datenschutz, aber konsequent» ist das Pendant, für das sich der Datenschutzbeauftragte auch bei der Digitalisierung einsetzt.

Auch die digitalen Bürgerinnen und Bürger wollen, dass die Verwaltung ihre Daten schützt. Eine 2018 von der ZHAW im Auftrag der Staatskanzlei und des Vereins der Zürcher Gemeindeschreiber und Verwaltungsfachleute (VZGV) durchgeführte Studie¹ zeigt, dass die Bevölkerung bei E-Services das Merkmal «Datensicherheit und Datenschutz» neben dem Preis als sehr wichtig einstuft. Die Bedeutung von Datenschutz und Datensicherheit wird dabei umso stärker gewichtet, je vertraulicher die Daten sind.

Tatsächlich bearbeitet die Verwaltung nicht nur eine riesige Menge an Daten, sondern auch immer mehr sehr sensitive Daten. Davon sind alle Bürgerinnen und Bürger betroffen – im Gesundheitswesen oder im Bildungsbereich. Sensitiv sind aber auch die Datenbearbeitungen im Bereich des Kindes- und Erwachsenenschutzes oder bei der Polizei und der Strafverfolgung. Der Datenschutzbeauftragte beschäftigte sich 2018 mit einer grossen Anzahl an Fragen aus diesen Gebieten [\[Seite 18\]](#).

Herausforderung Datensicherheit

Kontrollen und Prüfungen in unterschiedlichen Verwaltungsbereichen, bei Gemeinden, Spitälern und bei IT-Dienstleistern für die Verwaltung zeigten, dass die Sicherheit der Daten in der Digitalisierung eine grosse Herausforderung darstellt. Bis jetzt konnte noch keine nachhaltige Verbesserung der Informationssicherheit bei den öffentlichen Organen festgestellt werden [\[Seite 23\]](#).

Dabei wird der Austausch der Daten – auch über die Landesgrenzen hinweg – zur Selbstverständlichkeit: Verwaltungen speichern ihre Daten in der Cloud und nehmen Dienstleistungen in Anspruch, die in der Cloud erbracht werden. Die rechtlichen, organisatorischen und technischen Massnahmen zum Schutz der Daten sind komplex und oft ist es schwierig, mit allen Dienstleistern die offenen Fragen zu besprechen. Teilweise nutzen öffentliche Organe Standardprodukte wie Messenger-Dienste, ohne sich Gedanken zu machen über die damit zusammenhängenden Fragen des Datenschutzes und der Datensicherheit [\[Seite 30\]](#).

¹ Zürcher Hochschule für Angewandte Wissenschaften (ZHAW), Bedarfserhebung Digitales Leistungsportfolio bei Zürcher Gemeinden, Winterthur 2018 (ISBN 978-3-03870-023-4).

Schutz der Freiheitsrechte

Bei der Konzipierung der Digitalstrategie wie auch bei den in die Wege geleiteten Gesetzesrevisionen wird der Schutz der Freiheitsrechte der Bürgerinnen und Bürger zu wenig berücksichtigt (Seite 36). Die digitale Verwaltung ist aber auf das Vertrauen der Bürgerinnen und Bürger angewiesen. Ihr Vertrauen gründet auf dem Schutz ihrer Privatsphäre, also dem Datenschutz und dem sicheren Umgang mit ihren Daten.

Der Einsatz des Datenschutzbeauftragten für die Grundrechte der Bevölkerung stösst aber an Grenzen. Er kann die gesetzlichen Aufgaben mit den heutigen Ressourcen überall nur zum Teil wahrnehmen. Die Nachfrage nach Beratungen übersteigt die Möglichkeiten der Behörde und in Projekten und bei Ausbildungstätigkeiten kann er nur beschränkt mitwirken. Seit Jahren fehlen die Ressourcen für eine nachhaltige Kontrolltätigkeit, obwohl sich immer wieder grosse Lücken bei der Informationssicherheit zeigen. Das Plenum des Kantonsrats hat in der vergangenen Legislaturperiode eine Ressourcenaufstockung trotzdem zweimal abgelehnt.

Datenschutzaufsicht beim SIS

Das Schengen-Informationssystem (SIS) ist das Fahndungssystem der EU.

Die Schengen-Assoziierung ermöglicht seine Nutzung auch den Schweizer Polizeien, auch im Kanton Zürich. 2018 wurden über 19 000 Treffer mit Bezug zur Schweiz registriert. Ohne SIS wäre die Schweizer Polizei blind, bemerkte ein Vertreter der Bundespolizei. Die erfolgreichen Fahndungssysteme brauchen auch einen klaren datenschutzrechtlichen Rahmen. Die EU als Eigentümerin des SIS evaluiert in den angeschlossenen Ländern regelmässig, ob die datenschutzrechtlichen Vorgaben eingehalten werden. Die Evaluation in der Schweiz im Jahr 2018 hat zu verschiedenen Empfehlungen in Bezug auf die Datenschutzbehörden geführt, für deren Umsetzung die Schweiz einen Aktionsplan erstellen muss. Die Empfehlungen verlangen, dass die Durchsetzungsbefugnisse der Datenschutzbehörden gestärkt werden. Ihnen soll das Recht verliehen werden, direkt rechtsverbindliche Entscheidungen zu treffen.

Ebenso wird verlangt, dass den Datenschutzbehörden ausreichende finanzielle und personelle Mittel zur Verfügung gestellt werden, damit sie ihre Kontrollaufgaben im Rahmen des SIS wahrnehmen können. Dabei geht es um eine regelmässige Kontrolle der Rechtmässigkeit der Datenbearbeitungen im SIS.

Mit der Revision des Informations- und Datenschutzgesetzes (IDG) sollen im Kanton Zürich die Kompetenzen des Datenschutzbeauftragten gestärkt werden (Seite 37). Aufgrund mangelnder Ressourcen konnte in den letzten zehn Jahren im Kanton Zürich nur eine einzige Kontrolle der Datenbearbeitungen im SIS durchgeführt werden.

Digitalisierung braucht Ressourcen

Die Verwaltungsausgaben für die Datenbearbeitungen sind in den letzten Jahren stetig gestiegen. Der Regierungsrat stellt für die Verwaltung zusätzliche personelle Ressourcen und finanzielle Mittel in Millionenhöhe zur Verfügung, um der Digitalisierung den notwendigen Schub zu verleihen. Es ist nicht konsequent, wenn der Kantonsrat einerseits diese Aufstockungen genehmigt und andererseits die Anliegen eines angemessenen Datenschutzes ablehnt.

Ohne zusätzliche Ressourcen für den Datenschutzbeauftragten – dem Kompetenzzentrum für Datenschutz des Kantons Zürich – wird die Digitalisierung aber zu einem nicht einschätzbaren Wagnis für die Bürgerinnen und Bürger. Die Informatiksysteme werden komplexer und die Abhängigkeit von der Informationstechnologie nimmt zu, was die Cyber Risiken und die Gefahr des Missbrauchs von persönlichen Daten und digitalen Identitäten wachsen lässt. Die notwendigen Risikoabschätzungen werden nicht vorgenommen und die Technologien kaum auf ihre Datenschutzfreundlichkeit geprüft. Vorabkontrollen bei der Planung von Datenbearbeitungen und Kontrollen von bestehenden System sind Präventionsmassnahmen und gehören zu den Aufgabefeldern des Datenschutzbeauftragten. Dieser präventive Datenschutz ist aktuell aber nicht gewährleistet.

Defizite in der Aufgabenerfüllung

Das Jahr 2018 hat gezeigt, dass der Datenschutzbeauftragte die neue Dynamik der Digitalisierung nicht ohne Weiteres aufnehmen kann. Um in diesem Bereich die datenschutzrechtlichen Interessen der Bürgerinnen und Bürger geltend machen zu können, braucht es einen umfassenden Check-and-Balances-Prozess: Rechtliche, organisatorische und technische Anforderungen zum Schutz der Daten und ihrer Sicherheit müssen rechtzeitig und angemessen in die Digitalisierungsprojekte eingebracht werden können.

So liegt die Priorität auch beim Datenschutzbeauftragten im Bereich der Digitalisierung. Hier fallen heute die Entscheidungen darüber, wie die Verwaltung die Daten der Bürgerinnen und Bürger in Zukunft bearbeiten wird. Dabei müssen auch die Sicherung von Grundrechten und die Einhaltung gesetzlicher Bestimmungen zu den Zielvorgaben gehören. Dafür muss der Datenschutz von Anfang an mitgedacht werden. Doch die Konzentration auf die Digitalisierungsfragen darf nicht dazu führen, dass all die übrigen Datenbearbeitungen in der Verwaltung keine datenschutzrechtliche Begleitung mehr erhalten.

Die erwähnte Studie zeigt: Die Erwartungen der Bevölkerung in Bezug auf den Schutz und die Sicherheit ihrer vom Staat bearbeiteten Daten sind eindeutig. Es liegt an der Politik, die richtigen Weichen zu stellen.

Leistungsindikatoren im KEF

Die für das Jahr 2018 festgelegten Indikatoren im Konsolidierten Entwicklungs- und Finanzplan (KEF) weisen auf eine zunehmende Überlastung der Kapazitäten des Datenschutzbeauftragten hin.

Mit den bestehenden Ressourcen können etwa 500 Beratungen pro Jahr durchgeführt werden. Dieser Wert wurde 2018 um 20 Prozent überschritten. Die Beratungen im Kontext mit Digitalisierungsprojekten der Verwaltung werden zudem anspruchsvoller und aufwendiger. Die hohe Leistungsbereitschaft der Mitarbeitenden ermöglichte es, diesen Zusatzaufwand zu leisten. Um die Bedürfnisse der öffentlichen Organe und der Bürgerinnen und Bürger auch in diesem Bereich in Zukunft erfüllen zu können, braucht der Datenschutzbeauftragte zusätzliche Ressourcen.

Mit einem Monitoring stellt der Datenschutzbeauftragte sicher, dass er bei allen massgeblichen Vernehmlassungen einbezogen wird. Bei dieser Messgrösse wird von einer Mischung aus mehr oder weniger zeitaufwendigen Vernehmlassungsvorlagen ausgegangen. Im Berichtsjahr erfolgten quantitativ weniger Vernehmlassungen, dafür war zu Vorlagen von grosser Bedeutung Stellung zu nehmen, wie der IDG-Revision, der Totalrevision des Sozialhilfegesetzes oder den Leitlinien der Konferenz der Kantonsregierungen (KdK) zur Digitalen Verwaltung. Ihre Bearbeitung beanspruchte entsprechend viele Ressourcen.

Der Datenschutzbeauftragte bietet zahlreiche Weiterbildungen an, oft in Zusammenarbeit mit Ausbildungspartnern. Im Rahmen einer Zusammenarbeit mit der ZHAW werden verschiedene Seminare durchgeführt. Weitere Kurse, Seminare und Referate ergänzen diese Aktivitäten. Im Jahr 2018 ist der neue CAS Datenschutzverantwortliche an der ZHAW besonders zu erwähnen.

Aufgrund mangelnder Ressourcen kann die Kontrolltätigkeit nicht im vorgesehenen Ausmass durchgeführt werden. In der ersten Jahreshälfte erfolgten Nachkontrollen und in der zweiten Jahreshälfte wurden mehrere vertiefte Datenschutzreviews gestartet, die mit grösserem Aufwand verbunden sind.

Die Indikatoren zeigen, dass die gesetzlichen Aufgaben des Datenschutzbeauftragten kurz- und mittelfristig nur mit zusätzlichen Ressourcen zu bewältigen sein werden. Die umfassende Digitalisierung der Verwaltung in den nächsten Jahren wird zudem zu einer stark steigenden Nachfrage nach den Dienstleistungen des Datenschutzbeauftragten wie Beratung und Vorabkontrollen führen. Gerade vor dem Hintergrund der fortschreitenden Digitalisierung bleiben auch die übrigen gesetzlichen Aufgaben wie Information sowie Aus- und Weiterbildung wichtig.

Leistungsindikatoren		KEF	2018
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	600
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	14
Weiterbildung und Information	Der DSB bietet Aus- und Weiterbildungen im Bereich des Datenschutzes und der Informationssicherheit an. Dies erfolgt in der Form von internen oder externen Seminaren, Kursen, Workshops, Web-Trainingsprogrammen und Referaten. Der Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote für öffentliche Organe.	20	30
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	25