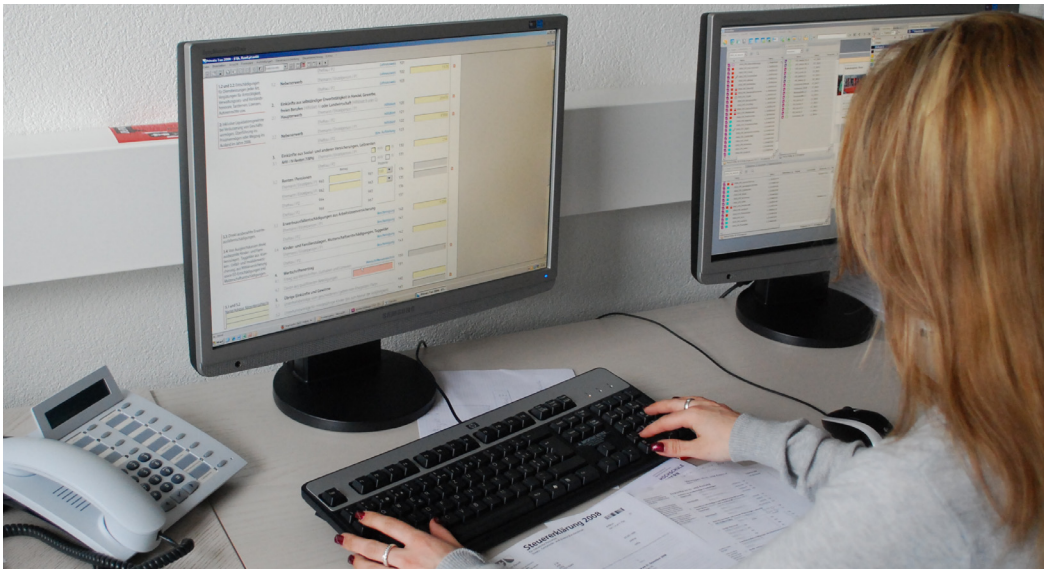
Die Verwantwortung liegt bei der Exekutive

Die Umsetzung der eGovernement-Strategie Schweiz bringt für Gemeinden auch Risiken mit sich. Sie müssen sicherstellen, dass elektronische Daten sicher aufbewahrt und übertragen werden. Die Verwantwortung für den Datenschutz liegt letztlich bei der Exekutive. Von Lukas Fässler*



Sicherheitstechnisch anspruchsvoll: Wenn beispielsweise Steuerinformationen elektronisch an die Gemeinde übermittelt werden, ist der Datenschutz gefordert. *Bild: Marcel Müller*

In den vergangenen Monaten wurden die wesentlichen Eckpunkte der eGovernment-Strategie Schweiz auch auf kommunaler Ebene erkannt. In den meisten Kantonen sind Registerharmonisierungsgesetze in Kraft getreten, in denen neben zusätzlichen Erfassungs- und Bewirtschaftungsaufgaben in den Subjektdaten auch der Datenaustausch zwischen den Gemeinden und den Kantonen geregelt wurden.

Viele kantonale Regierungsprogrammen enthalten mittlerweile eGovernment-Umsetzungsziele. Die Kantone evaluieren und implementieren derzeit Datenplattformen für den Austausch von Subjekt-, Objekt- und Finanzdaten und rüsten sich damit für die Aufgaben, welche sie in der öffentlich-rechtlichen Rahmenvereinbarung vom 29. August 2007 mit dem Bund übernommen haben. Die Kantone sind verpflichtet, die drei Hauptzielsetzungen der e-Government-Strategie Schweiz konsequent umzusetzen.

Danach wickelt die Wirtschaft den Verkehr mit den Behörden elektronisch ab, die Behörden haben ihre Geschäftsprozesse zu modernisieren und verkehren untereinander elektronisch und die Bevölkerung kann die wichtigen Geschäfte mit den Behörden ebenfalls elektronisch abwickeln.

Es ist aufgrund des Kataloges priorisierter Vorhaben bekannt, welche Prozesse, Daten und Schnittstellen in Zukunft von entscheidender Bedeutung sein werden, damit das Hauptziel des «medienbruchfreien Datenaustausches» erreicht werden kann. Die Exekutivmitglieder müssen nun – gestützt auf den Katalog priorisierter Vorhaben – überlegen, wo sie in ihren Prozessen und in ihrer Datenbewirtschaftung Änderungen vornehmen müssen. Zu beachten ist, dass dieser Katalog dauernd angepasst und erweitert werden kann, also eine stetige Auseinandersetzung mit ihm gefordert sein wird. Diese Verantwortung kann nicht einfach auf die Informatik und die Verantwortlichen für die Informatik in den Städten und Gemeinden delegiert werden.

Wer ist «Herr der Daten»?

Es liegt auf der Hand, dass die e-Government-Strategie Schweiz erhebliche Veränderungen in den kommunalen Prozessen zeitigen wird. Es werden neue Daten erhoben, bearbeitet, gespeichert, weitergeleitet, empfangen, validiert und wiederum ins kommunale System integriert werden müssen. Es wird geteilte Eigentümerschaften an Daten geben, da verschiedene Datenherren mit den Daten arbeiten werden. Deshalb wird es unumgänglich sein, sich im Rahmen der Umsetzung der e-Government-Strategie dauernd zu fragen, wem die aufbereiteten, zur Verfügung gestellten und wieder übernommenen Daten von ihrem Ursprung, ihrer gesetzlichen Grundlage und der primären Bewirtschaftungsaufgabe her gehören.

Die Frage nach dem Datenherrn wird zur zentralen Berechtigungsfrage. Wer nicht Datenherr ist, darf an den Daten nichts ändern, sondern diese nur übernehmen, allenfalls in seinem eigenen Bereich weiterbearbeiten. Dafür braucht der Übernehmer aber eine gesetzliche Grundlage. Die Gemeinden und Städte werden vorab im Bereich der Subjektdaten als Datenherren auftreten, weil sie die primäre Aufgabe der Erfassung, Verwaltung und Löschung von Einwohnerdaten als gesetzli-

** Lukas Fässler ist Rechtsanwalt und Informatikexperte. Er steht dem Verein Schweizerische Städte- und Gemeinde-Informatik (SSGI) als Präsident vor.*

che Aufgabe gefasst haben (Zivilstandsregister, Einwohnerregister, Todesregister etc.).

Datenschutz bei Transaktionen

Die Daten werden über Kommunikationsnetze und Infrastrukturen ausgetauscht, bereitgestellt und entgegengenommen. In diesem sogenannten Transaktionsbereich spielen vorab Fragen des Datenschutzes und der Datensicherheit eine wesentliche Rolle. Die Exekutivmitglieder stehen in der Verantwortung, im Rahmen der Umgestaltung und der Anwendung der neuen Prozesse, der Bearbeitung sowie der Übermittlung von Daten alle bestehenden Sorgfaltspflichten zu beachten. Wenn sie diese Sorgfaltspflichten ausser Acht lassen, nehmen sie ihre Verantwortung nicht wahr und müssen für allfällige Fehle oder Schäden gerade stehen.

Immer stärker wird die Pflicht gegenüber den Gemeinden durchgesetzt werden, künftig kein Papier mehr zu liefern. Es ist damit primäre Aufgabe der Exekutive, dafür zu sorgen, dass die Verwaltung ihre Prozesse neu ausrichtet. Die Prozesse müssen definiert, allseits bekannt und deren Einhaltung periodisch überprüft werden (Auditierung). Die Exekutivmitglieder müssen auch mitbestimmen, welche Anforderungen an solche Austauschportale gestellt werden. Die Portale sind vor unberechtigten Zugriffen Dritter zu schützen und der Missbrauch von Daten ist auszuschliessen. Dafür braucht es Vorgaben der Exekutive, welche die Mindestanforderungen an den sicheren und datenschutzkonformen Austausch von Daten festlegt. Diese Vorgaben können wiederum nicht vom Informatikchef einer Kommune vorgegeben werden, sondern müssen von der Führung kommen. Die Exekutive steht in der Verantwortung, die von ihr erlassenen Prozessvorgaben auf Einhaltung zu überprüfen. Vertrauen ist gut, Kontrolle ist besser und im Falle von datenschutzrelevanter Datenhaltung und dem dazugehörigen Datenaustausch sogar gesetzliche Pflicht.

Deshalb ist es wichtig, dass sich die obersten Verwaltungsbehörden regelmässig darüber Rechenschaft geben, ob die Verwaltung ihre Prozesse beherrscht, diese Prozesse überhaupt noch richtig sind, und welche Anforderungen an die Applikationen, die Datenhaltung oder die Auslagerung des Informatikbetriebes zu stellen sind. Die Verwaltung sollte sich dazu von Zeit zu Zeit unbedingt unabhängige Meinungen anhören, indem sie zum Beispiel einen Sicherheitsaudit machen lässt oder durch unabhängige Spezialisten etwa einen Hackerangriff simulieren lässt. Es empfiehlt sich aus Haftungsgründen unbedingt, die Ergebnisse solcher internen oder externen Prüfungen sowie die jährliche Überprüfung der Infrastrukturen in entsprechenden Beschlussprotokollen festzuhalten und die beschlossenen Massnahmen zu dokumentieren.

Entsprechende Protokolle sollten revisions- und beweistauglich in gesetzeskonformen Langzeit-Datenarchiven aufbewahrt werden und nicht verändert werden können. Der Einsatz von digitalen Signaturen und eines Langzeit-Archivs ist Voraussetzung dafür, dass die Behörde im Streitfall Beweise vorbringen kann, die anerkannt werden. Das gilt auch für die zweite (Daten) und dritte (Schnittstellen) Ebene der e-Government-Umsetzungs-Strategie.

Portale allein reichen für den Datenaustausch noch nicht aus, es braucht Applikationen, welche die Daten erfassen und bewirtschaften, es braucht Programme, welche den Austausch steuern und es braucht insbesondere Datenspeicher, welche die in der Hoheit der Gemeinde liegenden Daten rechtskonform aufbewahren. Dabei sind vorerst die Speicherung der vorhandenen Daten, der Zugriff auf diese Daten und die Berechtigungen für die Benutzung von Applikationen zu regeln.

Exekutive muss bei Pannen geradestehen

Auch wenn die Exekutive nicht im Detail wissen muss, wer mit welcher Applikation welche Daten bearbeitet, die Augen vor diesen Abläufen und den damit verbundenen Zuständigkeiten und dem nötigen Regelungsbedarf kann die Exekutive nicht verschliessen. Sie steht letztlich in der Verantwortung und muss den Kopf hinhalten, wenn in einer Gemeinde Daten über Einwohner an Dritte gelangen oder von Dritten entwendet werden, die dazu nicht berechtigt sind. Die Exekutive kann diese Aufgaben an ihre verantwortlichen Spezialisten wie interne Informatikleiter oder externe Rechenzentrumsanbieter übertragen. Dies ist von der Führungsverantwortung her zulässig. Was mit der Delegation der Aufgabe aber nie einhergeht, ist die gleichzeitige Delegation der Verantwortung. Diese bleibt immer bei der Exekutive hängen.

Das Öffentlichkeitsprinzip hat im Bezug auf die Datenhaltung und die Reproduzierbarkeit von Dossiers, Entscheiden, Unterlagen und Entscheidbeilagen eine dramatische Veränderung für die Verwaltung gebracht. Sofern eine Information nicht ausdrücklich als vertraulich oder geheim klassifiziert ist, hat der Bürger oder das Unternehmen grundsätzlich einen (klagbaren) Anspruch auf Bereitstellung, Einsichtnahme und Herausgabe von solchen Informationen. Mithin stellt es eine Sorgfaltspflicht der Exekutive dar, alle Informationen innerhalb eines Gemeinwesens zu klassifizieren, diese sauber aufzubewahren und im Falle einer Anfrage innert nützlicher Zeit liefern zu können.

SSGI strebt gemeinsame Lösungen an

Es hat keinen Sinn, wenn jede Gemeinde diese Anforderungen im Alleingang formuliert oder definiert. Der Verein SSGI bietet darum die Möglichkeit, in Arbeitsgruppen Lösungen für diese sensiblen Bereiche zu erarbeiten.

Der Verein hat in den Zielsetzungen 2009 unter anderem auch die Erarbeitung von Grundlagen für ein umfassendes Records-Management (Informationsverwaltung) mit Definition von Anforderungen an die Zwischenarchivierung, die beweistaugliche Langzeitarchivierung sowie die historische Datenarchivierung in Aussicht gestellt. Im übrigen arbeitet der Verein an einem Framework (Werkzeugkasten) von Grundsätzen und Weisungen, welches den Gemeinde-Exekutivmitgliedern helfen soll, ihre Sorgfaltspflichten wahrzunehmen und die notwendigen Grundsatzdefinitionen vorzunehmen. Schliesslich gehört auch die Sicherstellung eines jährlichen Reportings im gesamten Datenschutz- und Datensicherheits-Bereich dazu. ■