Aufgeklärte Bürger

von Lukas Gundermann

Im Zusammenhang mit der Einführung von e-Government kommt dem Thema Datenschutz in den Verwaltung eine immer größere Rolle zu. Behörden tun gut daran, sowohl im Front- als auch im Backoffice geeignete Maßnahmen zu ergreifen.

Das Grundsätzliche zuerst: Indem sich die Verwaltungen nach außen öffnen, entstehen im Frontoffice Gefährdungen für die Datensicherheit. Diesen Risiken muss durch technische Schutzmaßnahmen wie Firewalls begegnet werden. Bei der Übertragung personenbezogener Daten in unsicheren Netzen sollte immer die Möglichkeit der Verschlüsselung genutzt werden. Auf der Ebene der Anwendung besteht die Gefahr, dass im Rahmen von Transaktionen Daten der Bürger an Unberechtigte gelangen. Dies droht vor allem dann, wenn es den Bürgern möglich ist, unmittelbar auf ihre Daten zuzugreifen, oder wenn in bestimmte Verwaltungsprodukte Informationen einfließen, die in der Behörde schon vorliegen. Der Gefahr muss seitens der Behörden durch eine hinreichende Authentisierung der Bürger begegnet werden.

Daneben gibt es spezifische Risiken, die mit der Nutzung des Internets als Übertragungsweg einhergehen. Dazu gehört, dass technisch bedingt über jeden Besuch der Bürger auf dem Server der Behörde Daten über die Einzelheiten des Nutzungsvorgangs anfallen, die auf technischer Ebene protokolliert werden können. Allerdings untersagen die einschlägigen Regelungen, dass derartige Metadaten erhoben werden. Auch eine personalisierte Auswertung wäre mit den Datenschutzgesetzen nicht vereinbar. Geschäftsvorfälle im virtuellen Rathaus sollten also zurückhaltend protokolliert werden.

Vor dem Einstieg in die vollständige Online-Abwicklung von Verwaltungsleistungen sollte die ausdrückliche Einwilligung des Bürgers in die Nutzung dieses Kommunikationsweges eingeholt werden. Von Bedeutung ist weiterhin, dass die Bürger vollständig über die vorgesehene Datenverarbeitung aufgeklärt werden; Transparenz gehört zu den essentiellen Anforderungen des Datenschutzes.

Auch im Bereich Backoffice gibt es verschiedene Problemfelder. Aus technischer Sicht müssen Probleme der digitalen Archivierung gelöst werden: Welche Speichermedien sind möglichst resistent gegen Verfall und wie kann sichergestellt werden, dass die Daten auch in Jahrzehnten noch gelesen werden können – mit der dann aktuellen Hard- und Software? Werden elektronische Signaturen verwendet, muss geklärt werden, dass die erforderliche Nachsignatur der Dokumente sichergestellt ist. Wird dies unterlassen, verlieren die elektronischen Dokumente schon nach wenigen Jahren ihre Beweiskraft.

Mit der Einführung von elektronischen Akten geht häufig der Wunsch einher, die Datenhaltung zu zentralisieren und aus verschiedenen Anwendungen auf einheitliche Grunddaten der Bürger zuzugreifen. Solche Verfahren rufen die Datenschützer auf den Plan, weil sie das wichtige Prinzip der Zweckbindung in Gefahr sehen, wonach jedes Datum nur für den Zweck verwendet werden darf, für den es erhoben wurde. Gleichwohl muss damit eine zentrale Datenhaltung nicht per se ausscheiden. Es kommt allerdings darauf an, durch Beschränkungen der Zugriffsrechte jeder Stelle nur die Informationen zur Verfügung zu stellen, die sie für ihre Aufgabenerfüllung benötigt. Außerdem sollen

Web-Service

Von den Datenschutzbeauftragten des Bundes und der Länder wurde die umfangreiche Orientierungshilfe „Datenschutzgerechtes eGovernment“ erstellt. Sie steht im Internet zur Verfügung:

- **www.datenschutz.de**
- **www.lfd.niedersachsen.de**

Diese Links finden Sie auch unter www.kommune21.de.

die Daten vorrangig beim Betroffenen selbst erhoben werden. Willigt der Bürger allerdings ein, bereits einmal bei einer Kommune vorhandene Daten auch für andere Verfahren zu verwenden, so steht einer Datenübernahme nichts im Wege.

Die weitgehend oder ausschließlich elektronische Vorgangsbearbeitung bietet auch neue Chancen für den Datenschutz. Sucht eine andere Stelle um bestimmte Informationen nach, so muss nicht mehr die ganze Akte übersandt werden mit dem Hinweis, die anfragende Stelle möge sich die Fakten selbst heraussuchen. Gerade die datenbankmäßige Organisation der relevanten Informationen ermöglicht die gezielte Übermittlung nur der tatsächlich benötigten Daten, was übrigens auch gesetzlich gefordert ist. Weiterhin kann durch automatische Löschungen verhindert werden, dass umfangreiche Archive mit nicht mehr benötigtem Material entstehen. Wichtige Verfahrensschritte sollten aus Gründen der Rechtssicherheit und Nachweisbarkeit fälschungssicher protokolliert werden. Dies ermöglicht nicht nur eine nachträgliche Kontrolle auf Einhaltung der datenschutzrechtlichen Vorgaben, sondern ist auch schon aus verwaltungsverfahrensrechtlichen Gründen geboten.

Einige Themen sind übergreifend für Front- und Backoffice von Bedeutung. Die Datenschutzgesetze eröffnen die Möglichkeit, dass sich Behörden bei der Datenverarbeitung technisch versierter Spezialisten bedienen. Dabei muss allerdings der so genannte Auftragsdatenverarbeiter sorgfältig ausgewählt werden; in einem schriftlichen Vertrag ist seine Tätigkeit zu beschreiben. Dabei soll auch festgelegt werden, dass sich der Auftragnehmer den von der auftraggebenden Stelle veranlassten Kontrollen unterwirft. Diese muss ein eigenes Interesse daran haben, für die Rechtmäßigkeit und Datensicherheit beim Auftragnehmer zu sorgen, denn sie bleibt für die Datenverarbeitung verantwortlich.

Ein wichtiges Sonderproblem bei der Gestaltung vieler e-Government-Prozesse ist die notwendige Authentisierung der Bürger. Zwar hat der Bundesgesetzgeber im novellierten Verwaltungsverfahrensgesetz vollständig auf qualifizierte elektronische Signaturen gesetzt, die die Schriftform im Verwaltungsverfahren ersetzen sollen. Gleichwohl ist Skepsis angebracht. So ist schon aus Kostengründen nicht zu erwarten, dass sich qualifizierte Signaturzertifikate in der Bevölkerung in den nächsten Jahren nennenswert verbreiten. Ein weiteres Problem ist die mangelnde Interoperabilität der Signatur-Anwendungen. Dazu kommt, dass auch ein qualifiziertes Zertifikat nicht zur eindeutigen Identifikation herangezogen werden kann, da erforderliche Angaben wie Wohnort oder Geburtsdatum darin nicht enthalten sind. Auf Seiten der Signierenden bildet die elektronische Signatur nicht alle Funktionen der Schriftform ab; insbesondere kann es an der Warnfunktion im Hinblick auf rechtsrelevante Erklärungen fehlen.

Es müssen also andere Mechanismen zur hinreichend sicheren Authentisierung gefunden werden. In Betracht kommt etwa Authentisierung durch Abfragen von Zusatzinformationen, die ausschließlich dem Verfahrensbeteiligten bekannt sein sollten. Bei Anwendungen mit geringeren Gefahren für die Datenschutzrechte der Bürger wird es als Beleg für die Echtheit eines Antrags oft ausreichen, wenn eine korrekte Bezahlung der Verwaltungsleistung erfolgt ist. Als zusätzliche Absicherung bietet es sich an, einen kalkulierten Medienbruch vorzunehmen: Eine Zwischennachricht oder das Verwaltungsprodukt selbst sollte in Papierform an die Meldeadresse des Bürgers geschickt werden. So wird nicht nur die Datensicherheit erhöht. Wegen der Vertrauenskultur im Zusammenhang mit Papierdokumenten wird so zugleich zum stärkeren Vertrauen des Bürgers in die (dann eben nur halb-)elektronische Abwicklung beigetragen. Eine grundsätzliche Alternative zu Signaturen stellt ein so genanntes single sign on dar, wie es von Hamburg auf seiner neuen e-Government-Plattform realisiert werden wird.

Datenschutz: Kernpunkt beim e-Government.

Lukas Gundermann ist der für e-Government zuständige Referent beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein in Kiel.