Vorbeugen statt Heilen

Die zunehmende Leistungsfähigkeit der Fachverfahren und die Vernetzung der öffentlichen Verwaltungen stellen den Datenschutz vor neue Herausforderungen. Erfolgreiche Lösungsansätze kombinieren organisatorische und technische Maßnahmen.

Das Bundesverfassungsgericht hat die informationelle Selbstbestimmung als das Recht des Einzelnen definiert, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Die Grundsätze des Datenschutzes gelten auch für das elektronische Verarbeiten von Bürgerdaten. Relevant ist insbesondere die Zweckbindung, das heißt die Daten dürfen nur für den Zweck genutzt werden, für den sie erhoben wurden. Wichtig sind auch das Erforderlichkeit und Verhältnismäßigkeit, das heißt die Datenverarbeitung ist nur zulässig, soweit sie zur Aufgabenerfüllung notwendig ist. Darüber hinaus müssen die Daten vor Zugriffen Unbefugter geschützt und gegebenenfalls auch wieder gelöscht werden.

Ein Negativbeispiel ist hier die Arbeitsmarktreform Hartz IV: Die zur Leistungsberechnung genutzte Software A2LL ermöglicht es noch immer über 40.000 Mitarbeitern in der Bundesagentur für Arbeit und den ARGEn, bundesweit auf die Daten aller Leistungsempfänger zuzugreifen. Ein Berechtigungskonzept fehlt ebenso wie eine Löschkonzeption für falsche oder nicht mehr benötigte Daten. Die Datenschutzbeauftragte des Landes Thüringen, Silvia Liebaug, hat diese Mängel in ihrem Jahresbericht deutlich kritisiert. Dass es besser geht, zeigten die zwei optierenden Kommunen Thüringens. Sie nutzen zur Leistungsberechnung und Arbeitsvermittlung ein eigenständiges Verfahren. Zugriff zu den darin gespeicherten Daten der Arbeitssuchenden und Hilfeempfänger haben ausschließlich die Mitarbeiter des jeweiligen Grundsicherungsamts. Eine Übermittlung der Daten an andere Stellen erfolgt nicht.

Datenschutz: Bürger vertrauen der Verwaltung.

Die Rationalisierungsgewinne im E-Government – nicht nur im Rahmen der Hartz-IV-Prozesse – werden in erster Linie durch die Optimierung der Geschäftsprozesse im Back Office erzielt. Der Einsatz leistungsfähiger Fachverfahren und die fortschreitende interne und externe Vernetzung der Verwaltungen bedeuten eine Herausforderung für den Datenschutz. Johann Bizer, stellvertretender Landesbeauftragter für den Datenschutz in Schleswig-Holstein, hat dazu in einem Vortrag auf der Sommerakademie des Unabhängigen Landeszentrums für Datenschutz ausgeführt: „Das Primat der Infrastruktur hat Auswirkungen auf das Verhältnis zwischen Land und Kommunen: Die verwaltungsrechtliche Aufgabenteilung wird im E-Government überlagert durch die technisch-organisatorische Struktur aus Infrastruktur und Fachverfahren. Während die Organisationskompetenzen von Land und Kommunen in ihrem jeweiligen Bereich relativ konfliktfrei nebeneinander stehen, berührt die zentrale Gestaltung von Infrastruktur, wie etwa Active Directory, und Fachverfahren, wie Meldewesen, immer auch die Organisationskompetenzen jeder Verwaltungseinheit und damit ihre Zuständigkeit.“ Für den Datenschutz sei diese Frage fundamental, weil zu klären ist, wer gegenüber den Bürgern und Mitarbeitern die rechtliche

Verantwortung für die Verarbeitung ihrer Daten trägt. Besondere Probleme wirft nach Einschätzung von Bizer auch die Mächtigkeit einiger Fachverfahren auf. So lassen sich beispielsweise über Suchwerkzeuge Bürgerdaten jenseits von konkreten Zweckbindungen personenbezogen zusammenstellen. Bürgerdaten sind aber mehr als nur Mittel zum Zweck: Mit der Überlassung seiner Daten geht der Bürger davon aus, dass die jeweilige Verwaltungsstelle diese Daten nur für die Zwecke der konkreten Aufgabe verwendet. Ein weiterer Aspekt ist der Schutz der Mitarbeiterdaten, da jede Tätigkeit am elektronischen Arbeitsplatz protokolliert und diese Daten personenbezogen ausgewertet werden können. Diese Protokolldaten dürfen nicht zu Zwecken einer Leistungs- und Verhaltenskontrolle verwendet werden.

Die Einhaltung der Grundsätze des Datenschutzes sind von der Wahl der IT-Systeme und der Konzeption der Systemarchitektur abhängig. Deshalb rät das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein den Kommunen, bereits im Vorfeld größerer IT-Projekte Datenschutz-Experten beratend einzuschalten. Ob Fachverfahren oder Internet-Anbindung: Anforderungen der Datensicherheit sind für die Systemplanung, die Beschaffung, die Implementierung und den Betrieb zu beachten. Dabei erfüllen die Maßnahmen der Datensicherheit eine doppelte Funktion: Sie dienen dem technischen Schutz personenbezogener Daten, aber auch der Ordnungsmäßigkeit, das heißt einem geregelten und funktionsgerechten Systembetrieb. Aus diesem Grund bedürfen IT-Verfahren eines IT- und eines Sicherheitskonzepts, in dem nach einer Beschreibung möglicher Schadensfälle die relevanten Maßnahmen beschrieben werden.

Die schleswig-holsteinischen Datenschützer vertreten den Ansatz eines „Datenschutzes durch Technik“, weil sie den Datenschutz nicht gegen die Technik, sondern mit ihr gestaltend in die Verfahren implementieren wollen. Ein Instrument des technischen Datenschutzes ist das Datenschutz-Gütesiegel aus Schleswig-Holstein. Es soll dazu beitragen, den Datenschutz in die Produkte bringen, damit die datenverarbeitenden Stellen den „Datenschutz inside“ bei den Anbietern von IT-Systemen erwerben können. Ein weiteres Instrument zur datenschutzkonformen Gestaltung des E-Government ist das Datenschutzaudit. Es handelt sich dabei um eine Methode, die Verfahren der Verwaltung zu prüfen und die Datenschutzkonformität der Systeme zu bestätigen *(siehe S. 20)*. Auch interkommunale Kooperationen können dabei helfen, die nötigen Kompetenzen im Datenschutz aufzubauen *(siehe S. 18)*.

Ein wichtiger Aspekt des technischen Datenschutzes ist auch die Etablierung bundesweit einheitlicher Sicherheitsstandards. Erst kürzlich hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den flächendeckenden Aufbau einer OSCI-basierten Infrastruktur empfohlen. Beispielhaft und wegweisend sei in dieser Hinsicht der E-Government-Standard OSCI (Online Services Computer Interface), der eine durchgehende Sicherheit vom Versand bis zum Empfang einer Datenübermittlung gewährleistet. Eine derartige Ende-zu-Ende-Sicherheit habe den Vorteil, dass der Schutz der übermittelten Nachricht nicht von der Zuverlässigkeit der Boten, sondern der Sicherheit des Transportbehältnisses abhängig ist. Public Key Infrastrukturen (PKI) bieten darüber hinaus auch die Möglichkeit, sensible Daten innerhalb einer Kommune wirkungsvoll zu schützen *(siehe S. 22)*.

Doch die Herausforderungen für den Datenschutz sind nicht nur technologischer und organisatorischer Natur. Im so genannten Krieg gegen den Terror wachsen auch die Begehrlichkeiten von politischer Seite, Datenbestände jenseits der Zweckbindung etwa für Fahndungszwecke auswerten zu dürfen. Ende vergangenen Jahres hat der Landesbeauftragte für den Datenschutz Baden-Württemberg, Peter Zimmermann, deshalb vor einer Erosion des Datenschutzes gewarnt. Er sagte: „Dabei denke ich nicht nur an die zur Zeit auf europäischer Ebene geplante Vorratsspeicherung von Daten über elektronische Kommunikation, sondern auch an ähnliche Tendenzen hier in Deutschland.“ Ein Beispiel sei die Diskussion um die Öffnung von Mautdaten für Fahndungszwecke. Das Strickmuster ist dabei nach Meinung des Datenschutzbeauftragten oft ähnlich: „Zuerst wird nur für ganz bestimmte Zwecke eine neue Technik eingeführt; ist die Technik erst mal da, wird unter Hinweis auf die unausweichliche Notwendigkeit der Bekämpfung schwerster Straftaten der Verwendungszweck ausgedehnt.“ Auf diese Weise würden die individuellen Bürgerrechte stetig ausgehöhlt.

Rainer Hill