Voraussetzung für **Vertrauen**

von P. Schaar

Bei der Entwicklung von E-Government-Verfahren ist insbesondere die Einhaltung von Datenschutzaspekten zu berücksichtigen. Das heutige Datenschutzrecht stößt dabei jedoch an Grenzen.

Kaum ein E-Government-Verfahren kommt ohne die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus. Der Datenschutz ist dabei in erster Linie gefragt, wenn in den Verfahren Daten der Bürger verarbeitet werden. Häufig wird der Datenschutz als Hemmnis für den Einsatz effizienter Verfahren und Technologien in der Verwaltung wahrgenommen. Dieser Befund hält einer näheren Überprüfung jedoch kaum Stand. Die Gewährleistung des Datenschutzes ist vielmehr eine Voraussetzung für rechtssicheres Verwaltungshandeln – dies gilt für die klassische Verwaltung ebenso wie für elektronisches Behördenhandeln. Zudem werden Bürger und Unternehmen E-Government-Anwendungen nur dann nutzen, wenn sie ihnen das notwendige Vertrauen entgegenbringen und die datenschutzrechtlichen Standards nachweisbar eingehalten werden.

In der Praxis zeigt sich, dass viele E-Government-Anwendungen mit den herkömmlichen datenschutzrechtlichen Instrumenten angemessen begleitet werden können. Die zentralen Prinzipien der Erforderlichkeit, der Zweckbindung und der Transparenz gelten unabhängig von der zur Datenverarbeitung verwendeten Technik oder Organisationsmodellen. Gleichwohl werden bei der Planung und Umsetzung von E-Government-Vorhaben Grenzen des Datenschutzrechts deutlich, etwa bei der Überführung der klassischen Papierakte in digitale Vorgangsverwaltungssysteme. Dies liegt vielfach an einem allgemeinen Modernisierungsstau im Datenschutzrecht, welches konzeptionell noch aus den 1980er-Jahren stammt und deshalb einer grundlegenden Überarbeitung bedarf.

Auch wenn Datenschutz traditionell eher als juristische Materie betrachtet wird, nimmt die Bedeutung technologischer Aspekte stetig zu. Umso wichtiger ist es, Anforderungen des Datenschutzes bei der Entwicklung von E-Government-Verfahren und bei Entscheidungen über die Beschaffung und den Einsatz von IT-Systemen möglichst frühzeitig zu berücksichtigen (Privacy by Design). Neben der Gewährleistung der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) steht dabei die Datensparsamkeit im Vordergrund. Grundsätzlich sollten Systeme bevorzugt werden, bei denen keine oder so wenig wie möglich personenbezogene Daten anfallen. So ist es etwa für die Altersverifikation regelmäßig nicht erforderlich, den Namen und die Anschrift der Betroffenen festzuhalten. Die eID-Funktion des neuen Personalausweises enthält ein entsprechendes datenschutzfreundliches Feature. Aber auch wenn personenbezogene Daten erforderlich sind, um eine bestimmte elektronische Dienstleistung zu erbringen, bedeutet dies keineswegs, dass diese auf Dauer personenbezogen gespeichert werden müssen. Vielmehr ist dafür zu sorgen, dass die Daten möglichst frühzeitig gelöscht oder zumindest anonymisiert werden. Auch durch eine Pseudonymisierung personenbezogener Angaben lässt sich vielfach ein verbesserter Datenschutz erreichen. Eine gleichermaßen datenschutz- wie bürgerfreundliche Verwaltung sollte es daher ermöglichen, dass elektronische Verfahren so genutzt werden können, dass ohne Änderung der Voreinstellungen ein

E-Government braucht Datensparsamkeit.

möglichst weitgehender Schutz der persönlichen Daten gewährleistet ist (Privacy by Default).

Manche Verwaltungspraktiker betrachten gerade bei E-Government-Vorhaben die im Datenschutzrecht verankerte strikte Zweckbindung als hinderlich. Dies betrifft etwa die übergreifende Inanspruchnahme von Verwaltungsdienstleistungen bei zentralen E-Government-Portalen, die dadurch geprägt sind, dass in einem Front Office eine Vielzahl zu unterschiedlichen Zwecken erhobener personenbezogener Daten anfällt, während erst im Back Office die Differenzierung nach Aufgaben und Zwecken stattfindet. Daraus wird das Bedürfnis abgeleitet, zumindest bestimmte Stammdaten eines Bürgers zweckübergreifend zu nutzen, was auf Grundlage einer Einwilligung der Betroffenen ermöglicht wird. Dies stößt allerdings dann an Grenzen, wenn zum Zeitpunkt der Datenerhebung die zukünftigen Zwecke noch gar nicht feststehen. Der in diesem Zusammenhang immer wieder geforderten generellen Lockerung der Zweckbindung ist allerdings mit Vorsicht zu begegnen. Denn damit würde die Neigung zur vorsorglichen Speicherung personenbezogener Daten zunehmen. Zentrale strategische Überlegungen zum E-Government zielen außerdem zunehmend auf eine Bündelung von Aufgaben und eine ebenenübergreifende Kooperation von Behörden, was auch den Datenschutz tangiert. So gestaltet sich die gemeinsame Verarbeitung personenbezogener Daten durch unterschiedliche Behörden in einem Datenbestand selbst dann schwierig, wenn für die einzelnen Verarbeitungsschritte jeweils eine rechtliche Legitimation vorhanden ist. Dies hat sich exemplarisch beim Verfahrensmanagement Großraum- und Schwertransporte (VEMAGS) gezeigt. Die meisten Datenschutzgesetze in Bund und Ländern sehen nämlich eine solche gemeinsame Datenverarbeitung nicht vor, sodass häufig nur die Rechtsfigur einer Datenverarbeitung im Auftrag bleibt, welche aber einen hohen bürokratischen Aufwand erfordert. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb eine Mustervorschrift entwickelt, die eine solche gemeinsame Datenverarbeitung mit geringerem Aufwand ermöglicht und dennoch ein hohes Datenschutzniveau sichert.

Bei E-Government-Verfahren handelt es sich zudem häufig um äußerst komplexe IT-Anwendungen, bei denen insbesondere die Einhaltung der Datensicherheit nur mit hohem Aufwand kontrolliert werden kann. Umso wichtiger ist es, die verantwortlichen Stellen stärker in die Pflicht zu nehmen und Anreize für den Einsatz entsprechender Technologien zu schaffen. Dabei kann einer unabhängigen Zertifizierung von IT-Produkten und -Verfahren eine wichtige Rolle zukommen. Die Bundesregierung hat hierfür die Einrichtung einer Stiftung Datenschutz angekündigt – diese ist allerdings nur dann akzeptabel, wenn ihre strukturelle und finanzielle Unabhängigkeit sichergestellt wird und die Kompetenzen der Datenschutzbehörden unangetastet bleiben. Darüber hinaus müssen auch die internen Mechanismen zur Einhaltung des Datenschutzes gestärkt werden. Dazu gehört zum einen die Aufstellung verbindlicher Datenschutzkonzepte, denen eine Analyse der Risiken für die Persönlichkeitsrechte vorausgehen muss. Nicht zuletzt muss die Position der behördlichen Datenschutzbeauftragten weiter gestärkt werden, um eine effektive und regelmäßige interne Kontrolle auch komplexer IT-Anwendungen in der Verwaltung sicherzustellen.

Peter Schaar ist Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.