Datenschutz ist Verbraucherschutz

Das »informationelle Selbstbestimmungsrecht« gilt auch in sozialen Diensten und Einrichtungen

■ Helmut Kreidenweis

Ein bedeutsames Recht des Verbrauchers ist der Schutz seiner Daten. Nach den Bestimmungen des Bundesdatenschutzgesetzes und des Sozialgesetzbuches ist eine Speicherung personenbezogener Daten nur aufgrund gesetzlicher Bestimmungen oder nach der Einwilligung der Betroffenen erlaubt. In der praktischen Arbeit sozialer Organisationen stellen diese Auflagen eine besondere Herausforderung für das Management und für die Fachkräfte dar.

Datenschutz bezeichnet einerseits den Schutz personenbezogener Daten vor Missbrauch, andererseits den Schutz der Menschen vor unangemessenen Formen der Sammlung und Nutzung von Informationen zu ihrer Person. Beides ist zusammengefasst in dem vom Bundesverfassungsgericht 1983 geprägten, auf Art. 2 Abs. 1 des Grundgesetzes basierenden Begriff des »informationellen Selbstbestimmungsrechts«. Er steht für die grundlegende Idee, dass jeder Mensch selbst über seine Daten verfügen kann und ihm die Entscheidung obliegt, ob, wo und wie lange sie gespeichert werden. Schutzwürdige personenbezogene Daten dürfen grundsätzlich nur aufgrund von Gesetzen oder mit der ausdrücklichen Einwilligung der Betroffenen gespeichert und verarbeitet werden. Einschränkungen dieses Rechts sind nur in Notsituationen erlaubt.

Vom Datenschutz zu unterscheiden ist die Sicherheit in der Informationstechnologie (IT), auch Datensicherheit genannt. Die IT-Sicherheit umfasst technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes; zu ihren Aufgaben gehört jedoch die Sicherung sonstiger, also nicht gesetzlich geschützter Daten vor Verlust oder Missbrauch sowie die Gewährleistung eines reibungslosen Betriebs von IT-Systemen in Unternehmen.

Vom Datenschutz zu unterscheiden ist die Schweigepflicht. Diese ist im Strafgesetzbuch (StGB § 203) und häufig auch privatrechtlich in Arbeitsverträgen geregelt. Während hier die Frage der Weitergabe (»Offenbarung«) fremder, insbesondere personenbezogener Informationen im Mittelpunkt steht, geht es beim gesetzlichen Datenschutz vor allem um Fragen der Berechtigung zur Speicherung von Daten sowie deren Sicherung gegen Missbrauch.

Zentrale gesetzliche Grundlage für den Datenschutz ist das Bundesdatenschutzgesetz (BDSG), das ergänzt wird durch die Datenschutzgesetze der Bundesländer. Die in zahlreichen anderen Bundesgesetzen enthaltenen bereichsspezifischen Rechtsvorschriften haben Vorrang vor dem Bundesdatenschutzgesetz.

Die für soziale Organisationen wichtigsten sind in den Sozialgesetzbüchern (SGB) I und X enthalten. Daneben finden sich spezielle Vorschriften etwa im SGB II, V, VIII und XI. Teilweise sind die dortigen Bestimmungen an die Regelungen des Bundesdatenschutzgesetzes angelehnt oder verweisen darauf, teilweise gehen sie darüber hinaus oder schränken sie ein.

Insgesamt erweist sich die datenschutzrechtliche Situation für die Soziale Arbeit als komplex und wenig übersichtlich. Zum einen sind die Regelungen über verschiedene Gesetzeswerke des Bundes, der Länder und der Kirchen verstreut und uneinheitlich gegliedert. Zum anderen sind zentrale Begriffe wie »Betroffener« oder »verarbeitende Stelle« nicht definiert und geben so Anlass zu Interpretationen (vgl. Moersberger 1998, S. 28ff). Auch die Geltungsbereiche ganzer Gesetze sind etwa für Einrichtungen in der Trägerschaft kirchlicher Wohlfahrtsverbände strittig. Während die allgemeinen Vorschriften des Bundesdatenschutzgesetzes (§§ 1–11) unabhängig von der Art der verarbeitenden Organisation gelten, wird bei den speziellen Vorschriften zwischen öffentlichen Stellen (§§ 12–26) und nichtöffentlichen Stellen (§§ 27–38a) unterschieden. Daneben gibt es Bereiche, die

Prof. Helmut Kreidenweis ist Hochschullehrer für Sozialinformatik an der Katholischen Universität Eichstätt-Ingolstadt und Leiter der dortigen Arbeitsstelle für Sozialinformatik.
E-Mail helmut.kreidenweis@ku-eichstaett.de

vollständig aus dem Geltungsbereich des Bundesdatenschutzgesetzes herausgenommen sind.

Die vielgestaltige Struktur der sozialen Dienstleistungslandschaft macht die Zuordnung einer Einrichtung zu einem der Geltungsbereiche nicht immer leicht. Zum öffentlichen Bereich im Sinne des Bundesdatenschutzgesetzes zählen alle Einrichtungen des Bundes und der Länder. Auf Landes- und Kommunalebene gelten zusätzlich die Datenschutzgesetze der Länder. Öffentliche Stellen, die als öffentlich-rechtliche Unternehmen am freien Wettbewerb teilnehmen, zählen zum nichtöffentlichen Bereich. Darunter fallen beispielsweise kommunale Pflegeheime oder Jugendhilfe-Einrichtungen, die in ähnlicher Form auch von freigemeinnützigen oder privatwirtschaftlichen Trägern betrieben werden. Zum nichtöffentlichen Bereich gehören alle natürlichen und juristischen Personen, die Daten geschäftsmäßig oder für berufliche Zwecke nutzen. Damit sind neben allen freiberuflich Tätigen auch soziale Einrichtungen erfasst, die in Form von Vereinen (§ 21 BGB), Kapitalgesellschaften (z. B. GmbH, § 17 ff. HGB) oder Gesellschaften bürgerlichen Rechts (§§ 705 ff. BGB) organisiert sind. Soweit nicht-öffentliche Stellen hoheitliche Aufgaben in Delegation wahrnehmen, gelten für sie die Bundesdatenschutzgesetz-Bestimmungen des öffentlichen Rechts. Dies gilt für freie Träger, an die hoheitliche Aufgaben der Jugendämter aus dem Bereich des SGB VIII übertragen werden.

Im Bereich der verfassten Kirchen hat das Bundesdatenschutzgesetz keine Gültigkeit. Stattdessen gibt es eigene kirchliche Regelungen, die dem Bundesdatenschutzgesetz ähneln, jedoch nicht mit ihm identisch sind. Nicht abschließend geklärt ist, ob für soziale Einrichtungen in kirchlicher Trägerschaft sowie in Trägerschaft der kirchlichen Wohlfahrtsverbände das Bundesdatenschutzgesetz oder die kircheneigenen Bestimmungen gelten.

Über das Bundesdatenschutzgesetz hinaus regelt vor allem § 35 SGB I in Verbindung mit den §§ 67 bis 85 SGB X den Datenschutz für die Leistungsträger nach den Büchern des Sozialgesetzbuches. Zu den Leistungsträgern gehören u. a. die Krankenkassen, die Rentenversicherungsträger und die Jugendämter. Davon zu unterscheiden sind die Leistungserbringer wie ambulante oder stationäre Einrichtungen der freigemeinnützigen oder privatwirtschaftlichen Träger. Für diese gibt es nur in Teilen des Sozialgesetzbuches explizite Regelungen. Im Geltungsbereich des SGB VIII sagt der § 61 Abs. 4 hierzu: »Werden Einrichtungen und Dienste der Träger der freien Jugendhilfe in Anspruch genommen, so ist sicherzustellen, dass der Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung und Nutzung in entsprechender Weise gewährleistet ist.« Jugendämter als Leistungsträger haben demnach einen Sicherstellungsauftrag für den Datenschutz. Diesen müssen sie vertraglich, also beispielsweise in einer Leistungsvereinbarung geltend machen. Nimmt der Leistungsträger seinen Sicherstellungsauftrag wahr, so gilt der Sozialdatenschutz nach § 35 SGB I für die Einrichtungen der freien Träger entsprechend.

Was geschützt werden muss

Unmittelbar gilt für freie Träger nach § 78 Abs. 1 und 2 SGB X die Verpflichtung, Sozialdaten, die sie von einem Leistungsträger erhalten haben, geheim zu halten. Schutz nach den allgemeinen Bestimmungen des Bundesdatenschutzgesetzes (§§ 1-11) genießen alle Angaben über persönliche und sachliche Verhältnisse, die eindeutig einer natürlichen lebenden Person zugeordnet sind oder ihr zugeordnet werden können.

Einen Unterschied zwischen den Datenschutzvorschriften für den öffentlichen und den nichtöffentlichen Bereich macht das Bundesdatenschutzgesetz bei der Form der Datenverarbeitung: Im nichtöffentlichen Bereich gilt als Voraussetzung für die Schutzwürdigkeit das Vorliegen der Daten in einer automatisierten Datei, etwa einer Datenbank. Im öffentlichen Bereich erstreckt sich der Schutz auch auf aktenmäßig, also etwa auf Papier oder Mikrofilm erfasste Informationen.

Für den Datenschutz nach dem SGB I und X ist ähnlich den Regelungen des Bundesdatenschutzgesetzes für den öffentlichen Bereich die Form der Datenhaltung nicht von Belang. Hier genügt allein die Tatsache, dass solche Angaben in irgendeiner Form erfasst werden. Da für die Gewährung staatlicher Sach- oder Geldleistungen meist umfängliche Angaben über die persönlichen Verhältnisse erforderlich sind, enthält das Sozialgesetzbuch hierfür spezielle Datenschutzvorschriften. Sie gehen zum Teil über die Vorschriften des Bundesdatenschutzgesetzes hinaus oder präzisieren diese. In § 35 SGB I heißt es: »Jeder hat einen Anspruch darauf, dass Einzelangaben über seine persönlichen und sachlichen Verhältnisse (personenbezogene Daten) von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Die Wahrung des Sozialgeheimnisses umfasst auch die Verpflichtung, die technischen und organisatorischen Maßnahmen einschließlich Dienstanweisungen zu treffen, die erforderlich sind, um sicherzustellen, dass dem Sozialgeheimnis unterliegende personenbezogene Daten nur Befugten zugänglich sind.«

Die Offenbarung von Daten, die dem Sozialgeheimnis nach dem Sozialgesetzbuch unterliegen, ist in den §§ 67 bis 77 SGB X geregelt. Diese Daten dürfen nur dann weitergegeben werden, wenn der Betroffene eingewilligt hat oder wenn ein Gesetz dies erlaubt. Zu dieser gesetzlichen Offenbarungsbefugnis zählen unter anderem die Amtshilfe, die Erfüllung von Aufgaben nach dem Sozialgesetzbuch einschließlich eines damit zusammenhängenden gerichtlichen Verfahrens, die Abwendung geplanter Straftaten sowie der Schutz der öffentlichen Gesundheit. Erlaubt ist auch die Forschung, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden oder wenn das öffentliche Interesse das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt.

Wichtigste Grundsätze des gesetzlichen Datenschutzes (§ 3 BDSG) sind die Datenvermeidung und Datensparsamkeit. Gestaltung und Auswahl von Datenverarbeitungssystemen müssen sich an dem Ziel ausrichten, so wenig personenbezogene Daten wie möglich zu erheben. Insbesondere sollen Daten, wenn möglich, anonymisiert werden um der Rückschluss auf konkrete Personen zu vermeiden. Nach den Bestimmungen des Bundesdatenschutzgesetzes und des Sozialgesetzbuches ist eine Speicherung personenbezogener Daten nur aufgrund einer gesetzlichen Bestimmung oder der Einwilligung der Betroffenen erlaubt.

In der praktischen Arbeit sozialer Organisationen besteht oft keine gesetzliche Notwendigkeit für die Erfassung von Personendaten. Daher ist zu ihrer elektronischen Erfassung die ausdrückliche und

persönliche Einwilligung des Betroffenen erforderlich. Die Einwilligung muss immer vor der Datenerfassung erteilt werden, eine nachträglich erteilte Zustimmung hat keine legalisierende Wirkung. Für eine rechtsgültige Einwilligung gelten drei Voraussetzungen:

- Der Betroffene muss die Tragweite seiner Entscheidung erkennen können. Dies setzt voraus, dass er über den Zweck der Speicherung und gegebenenfalls der Übermittlung der Daten an Dritte hinreichend aufgeklärt wird.
- Die Einwilligung bedarf im Regelfall der Schriftform. Die Unterschrift muss vom Betroffenen eigenhändig im Original auf die Erklärung gesetzt werden.
- Wird die Unterschrift zusammen mit anderen Erklärungen erteilt, so ist der Betroffene darauf besonders hinzuweisen. Dazu muss die Einwilligung im Schriftbild etwa durch Einrahmung oder Fettdruck hervorgehoben werden.

Abweichungen von dieser Form der Einwilligung sind nur aufgrund von Eilbedürftigkeit, etwa in medizinischen Notfällen möglich. Nicht abgewichen werden kann, wenn der Betroffene aufgrund seines geistigen oder körperlichen Zustandes dazu nicht mehr in der Lage ist. Dann muss ein gesetzlicher Betreuer bestellt werden, der die Einwilligung stellvertretend erteilt. Bei Minderjährigen müssen die Erziehungsberechtigten die Einwilligung erteilen.

Werden Daten von Klienten oder Mitarbeitern mit deren Einwilligung erfasst, so sind sie an den Verwendungszweck im Rahmen eines bestehenden oder sich anbahnenden Vertragsverhältnisses gebunden. Eine Nutzung oder Weitergabe, die über diesen Zweck hinausgeht, ist nicht gestattet. Dabei dürfen nur Daten erhoben werden, die für die Zweckerfüllung erforderlich sind. Eine Datenerfassung »auf Vorrat«, also für einen unbestimmten oder in Zukunft liegenden Zweck, ist untersagt. Wenn Daten unrichtig sind, ihre Speicherung unzulässig war oder ihre Speicherung zur Zweckerfüllung nicht mehr erforderlich ist, verlangen die Datenschutzgesetze (§ 19 und 35 BDSG, § 84 SGB X) ihre Korrektur oder Löschung. An die Stelle einer Löschung tritt die Sperrung, wenn der Löschung gesetzlichen oder vertraglichen Aufbewahrungsfristen entgegenstehen, schutzwürdige Interessen des Betroffenen beeinträchtigt werden, eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen lässt.

Was Dienste und Einrichtungen veranlassen müssen

Um den Datenschutz zu gewährleisten, müssen alle Mitarbeiter mit Zugang zu schutzwürdigen Personendaten die einschlägigen Vorschriften kennen und ihr berufliches Handeln danach ausrichten. Der Gesetzgeber fordert vom Arbeitgeber, diese Mitarbeiter auf das Datengeheimnis zu verpflichten. Angehörige des öffentlichen Dienstes sind meist bereits aufgrund dienstrechtlicher Vorschriften zur Wahrung des Datengeheimnisses verpflichtet. In Organisationen privater Träger ist eine entsprechende Erklärung im Rahmen des Arbeitsvertrages üblich. Neben der Schweigepflicht sollte sie auch die fahrlässige Zugänglichmachung von Daten umfassen, wie sie etwa durch Unachtsamkeit bei der elektronischen Datenverarbeitung entstehen kann.

Um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten, verlangt das Bundesdatenschutzgesetz (§ 4 f.) von öffentlichen und nichtöffentlichen Stellen die Bestellung eines Beauftragten für den Datenschutz. Diese Pflicht besteht, wenn mindestens fünf Arbeitnehmer personenbezogene Daten automatisiert oder zwanzig Arbeitnehmer personenbezogene Daten auf andere Art verarbeiten. Zu seinen Aufgaben gehört die Überwachung der ordnungsgemäßen Anwendung aller Programme, mit denen personenbezogene Daten verarbeitet werden. Dazu muss er über Vorhaben zur Verarbeitung solcher Daten rechtzeitig unterrichtet werden. Eine weitere Aufgabe ist die Unterrichtung der Mitarbeiter über die Erfordernisse des Datenschutzes. Zur Erfüllung seiner Aufgaben müssen ihm die notwendigen Informationen zur Verfügung gestellt werden.

Besonderen Wert legt das Gesetz auf die Ernennung einer geeigneten Person. Um Interessenkonflikte zu vermeiden sollte der Datenschutzbeauftragte keine leitende Stellung einnehmen. In seiner Funktion soll er unmittelbar der Geschäftsleitung zugeordnet sein und über einschlägige Fachkenntnisse verfügen. Bei der Ausübung seiner Tätigkeit ist er nicht weisungsgebunden und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die zur Aufgabenerledigung erforderlichen Mittel wie Personal, Räume, Einrichtungen oder Geräte müssen ihm zur Verfügung gestellt werden. Diese Aufgabe kann auch einer externen Person übertragen werden, sofern sie die genannten Voraussetzungen erfüllt.

»Wichtigste Grundsätze des gesetzlichen Datenschutzes sind die Datenvermeidung und Datensparsamkeit«

War die Verarbeitung von Mitarbeiter-Daten in der Sozialwirtschaft bislang zumeist auf die Personalverwaltung beschränkt, rücken mit der Nutzung von Software für Fall- oder Pflegedokumentation vielfach neue Fragen des Datenschutzes ins Blickfeld, da solche Programme vielfach auch Informationen zu den betreuenden Mitarbeitern speichern. Dies sind beispielsweise Zeitpunkt und Dauer eines Beratungsgesprächs oder Inhalte einer pflegerischen Tätigkeit. Da solche Daten Rückschlüsse auf die Arbeitsleistung und das Verhalten einzelner Angestellter zulassen, greifen hier neben dem Bundesdatenschutzgesetz auch Regelungen im Betriebsverfassungsgesetz (BetrVG), im Bundespersonalvertretungsgesetz (BPersVG) und den Personalvertretungsgesetzen der Länder. Im öffentlichen Sektor gelten die Personalvertretungsgesetze und im privatwirtschaftlichen Bereich das Betriebsverfassungsgetz; die Bestimmungen sind inhaltlich weitgehend deckungsgleich. ▶

Nicht angewandt werden diese Bestimmungen nach geltender Rechtsprechung in den Kirchen und kirchlichen Wohlfahrtsverbänden. Doch auch die kirchlichen Arbeitsvertragsrichtlinien (AVR) enthalten Informations- und Mitspracherechte der Mitarbeitervertretungen. Darüber hinaus gibt es teilweise tarifvertragliche Regelungen oder Betriebsvereinbarungen zu Umgang mit Mitarbeiterdaten, die enger gefasst sein können als die gesetzlichen Normen. Da die Mitarbeiterrechte zum Datenschutz im Betriebsverfassungsgesetz und in den Personalvertretungsgesetzen als Beteiligungsrechte der Betriebs- oder Personalvertretungen formuliert sind, ist ihre Wahrnehmung an die Existenz eines Personal- oder Betriebsrates gebunden.

Resümee

Werden in sozialen Diensten und Einrichtungen personenbezogene Daten elektronisch verarbeitet, sind nach den Anlagen zu § 9 BDSG und § 78 a SGB X zahlreiche Maßnahmen zu treffen:

- **Zutrittskontrolle:** Unbefugten muss der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt sein.
- **Zugangskontrolle:** Unbefugten muss es unmöglich gemacht werden, Datenverarbeitungssysteme zu nutzen.
- **Zugriffskontrolle:** Auch wer berechtigt an Datenverarbeitungssystemen arbeitet, darf nur auf die Daten zugreifen können, für die er eine Zugriffsberechtigung hat. Es muss gesichert sein, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- **Weitergabekontrolle:** Es muss gewährleistet sein, dass personenbezogene Daten bei der elektronischen Übertragung, während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
- **Eingabekontrolle:** Es muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
- **Auftragskontrolle:** Es muss gewährleistet sein, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- **Verfügbarkeitskontrolle:** Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt sein.
- **Trennungskontrolle:** Die zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Für Sommer 2009 ist eine Novellierung des Bundesdatenschutzgesetztes geplant. Durch eine Verschärfung der Anforderungen zur Einwilligung der Betroffenen soll einem Datenmissbrauch im Bereich der Werbung vorgebeugt werden. Ebenso gestärkt werden soll die Stellung des Datenschutzbeauftragten in Unternehmen.

Der vorstehende Artikel ist die aktualisierte Fassung eines Lexikonbeitrags des Autors: Bernd Maelicke (Hg.): Lexikon der Sozialwirtschaft. Nomos Verlagsgesellschaft, Baden-Baden 2007. 1.128 Seiten. 98,– Euro. ISBN 978-3-8329-2511-6. ◆

Literatur

Gola, Peter; Schomerus; Rudolf; Klug, Christoph: Bundesdatenschutzgesetz (BDSG) Kommentar, 2005.

Gola, Peter; Jaspers, Andreas: Das Bundesdatenschutzgesetz im Überblick, 2005.

Moersberger, Thomas: Datenschutz und Datensicherheit für soziale Dienste. In: H. Kreidenweis u. a.: EDV 1998.

Tinnefeld, Marie-Theres; Ehman, Eugen: Einführung in das Datenschutzrecht im Sozialwesen. Kongress-Dokumentation COSA 97.

Internet-Quellen: http://www.bfd.bund.de – Bundesbeauftragter für den Datenschutz: Gesetzestexte.

Datenschutz-Hinweise für Unternehmen und Privatpersonen: http://www.datenschutz.de – Landeszentrum für Datenschutz Schleswig-Holstein: Informationen zu Recht und Technik.