Datenschutz

In nur wenigen anderen Bereichen werden so viele persönliche, sensible Daten erhoben, verarbeitet, gespeichert und weitergegeben wie in sozialen Diensten und Einrichtungen. Neben individuellen Mitarbeiterdaten sind davon unter anderem zu Behandlungs-, Beratungs- und Abrechnungszwecken auch geheimhaltungsbedürftige Informationen über Kunden, Klienten, Patienten und Bewohner betroffen.

Abb. 1: Zahlen zum Datenschutz

Heute erfolgt die Datenverarbeitung weitestgehend auf elektronischem Wege. Damit sind aber auch die **Risiken** im Datenschutz gestiegen (Abb. 1). Dass das Thema „Datenschutz" ein weites Feld ist, zeigen bereits einige Zahlen und Fakten. Im Zuge von Cyberkriminalität werden monatlich über 29 Millionen Datensätze weltweit gestohlen. Ein Großteil dieser Daten betrifft sensible Informationen. So ist es vielleicht nicht verwunderlich, dass über 62% der Deutschen nach neuesten Umfragen Bedenken bezüglich der Sicherheit ihrer Daten bei Unternehmen und Behörden äußern. Dies ist der zweithöchste Wert in Europa. Aber auch die Unternehmen selbst und deren Mitarbeiter können kostspielige Fehler im Datenschutz begehen. Geldbußen bis zu 300.000 Euro drohen für eine unbefugte Erhebung, Verarbeitung oder Weitergabe von Daten. Jeder einzelne von uns könnte aktiv am Schutz der eigenen Daten mitwirken. Aber nur etwa 29% der Deutschen haben in den letzten 12 Monaten das Passwort auf ihrem Computer oder Smartphone geändert.

Abb. 2: Inhalt der Unterweisung

Nachdem wir uns damit schon ein wenig mit der Bedeutung des Datenschutzes auseinandergesetzt haben, wenden wir uns zunächst den theoretischen Grundlagen zu, die für die praktische Umsetzung im Betrieb relevant sind. Daraus lassen sich allgemeine Kontroll-, Zutritts- und Zugriffsmaßnahmen ableiten.

Wie gestalten Sie Ihren Arbeitsplatz unter datenschutzrechtlichen Gesichtspunkten optimal? Wie verhalten Sie sich richtig im Internet und im Umgang mit Sozialen Medien? Was sollten Sie zum Thema Schweigepflicht wissen? Wie führen Sie vertrauliche Gespräche und Telefonate? Und schließlich sollten Sie sich ein wenig im Urheberrecht auskennen. Dieses gilt es zu bedenken, sobald Sie selbst aktiv eigene Beiträge veröffentlichen möchten, sei es in Broschüren, Plakaten oder im Web. In

diesem Zusammenhang spielt auch das Recht am eigenen Bild eine Rolle.

Zum Datenschutz gibt es eine Vielzahl gesetzlicher Regelungen und Bestimmungen. Es wäre an dieser Stelle müßig, darauf im Einzelnen einzugehen. Aber der unabhängige Politiker Jörg Tauss formulierte ganz zutreffend: „Datenschutz ist kein lästiges Anhängsel. Er ist keine überflüssige Bürokratie. Er ist Voraussetzung dafür, dass auch in der Informationsgesellschaft das Recht auf informationelle Selbstbestimmung durchgesetzt werden kann."

Abb. 3: Gründe für Datenerhebungen

Aus welchen Gründen dürfen überhaupt Daten erhoben werden (Abb. 3)? Grundsätzlich ist es nach dem Bundesdatenschutzgesetz verboten, überhaupt persönliche Daten zu erfassen. Es gibt aber zwei Ausnahmen:

- Zum einen erlauben oder verpflichten besondere gesetzliche Bestimmungen den Trägern zur Datenerhebung, zum Beispiel zu Abrechnungszwecken mit den Kranken- und Pflegekassen.
- Und zum zweiten können Daten über eine Person dann erhoben werden, wenn diese ausdrücklich zustimmt. Diese Zustimmung ist aber wieder selbst an bestimmte Umstände geknüpft; so kann sie auch in Einzelfällen von Betreuern oder Erziehungsberechtigten erteilt werden.

Aber selbst dann können Sie nicht einfach willkürlich Informationen sammeln. Die erhobenen Daten sollen immer **zweckgebunden** sein, d.h. sie müssen erforderlich sein, damit Sie Ihre Arbeit erfolgreich gestalten können. Damit einher geht das **Prinzip der Datenvermeidung**. Es sollen also so wenige Daten gesammelt werden, wie nur eben möglich. Im Berufsalltag ist diese Abwägung nicht immer ganz einfach.

Abb. 4: Maßnahmen zur Datensicherheit

Wie können Unternehmen sicherstellen, dass mit den erhobenen Daten verantwortungsvoll umgegangen wird? Wie kann vermieden werden, dass Daten nicht unbefugt manipuliert, entwendet oder an unbefugte Personen weitergegeben werden (Abb. 4)?

Zunächst werden Sie feststellen, dass Sie es in Ihrer Einrichtung mit **Zutritts- und Zugangskontrollen** zu tun haben werden. Damit ist beabsichtigt, dass nur diejenigen Mitarbeiter Zutritt zu den technischen Anlagen erhalten, die unmittelbar für die Datenverarbeitung verantwortlich sind. Der Zugang wird weiter eingeschränkt durch passwortgeschützte Bereiche. Mit der Zugriffskontrolle soll sichergestellt werden, dass Berechtigungen für einen Zugang zu personenbezogenen Daten nur dann erteilt werden, wenn für die betroffenen Mitarbeiter eine unmittelbare dienstliche Notwendigkeit dazu besteht. Ein Mitarbeiter der Buchhaltung benötigt z.B. keinen Zugang zur Krankheitsgeschichte von Bewohnern in einem Altenheim.

Die **Weitergabekontrolle** verfolgt das Ziel, dass Daten auf dem Transportweg nicht in die Hände von unbefugten Personen gelangen. Darunter fallen etwa die Vorschriften zum

Umgang mit E-Mails, mit denen wir uns noch beschäftigen werden.

Die **Eingabekontrolle** soll bewirken, dass nachträglich immer festgestellt werden kann, wer genau welche Daten erfasst und verändert hat.

Und die **Verfügbarkeitskontrolle** soll sicherstellen, dass Datenbestände umfassend gegen Zerstörung und Verlust geschützt sind. Darunter fällt z.B. die Erstellung von Sicherungskopien.

Abb. 5: Aufgaben des Datenschutzbeauftragten

Um die Belange des Datenschutzes kümmert sich der betriebliche **Datenschutzbeauftragte** (Abb. 5). Er ist in der Ausübung seiner Tätigkeit weisungsfrei und verfügt über entsprechendes rechtliches und technisches Fachwissen, um seinen Aufgaben nachzukommen. Dazu zählen unter anderem:

- Mitwirkung bei der Erstellung interner Richtlinien und Dienstanweisungen zum Datenschutz. Dazu wird auch der Kontakt zu Behörden und Verbänden aufrechterhalten.
- Der Datenschutzbeauftragte kann jederzeit in seinem Tätigkeitsfeld Kontrollen durchführen oder anordnen. Auch bei Kontrollen durch die Aufsichtsgremien kann er mitwirken.
- Insbesondere die Überwachung des Datenverkehrs im Zuge zunehmender elektronischer Verfahren bei der Erfassung und Weitergabe von Daten spielt hier eine wesentliche Rolle.
- Der Datenschutzbeauftragte informiert die Mitarbeiter über Gesetzesnovellen, über EU-Richtlinien, zum Persönlichkeitsrecht und zur Rechtsprechung zu datenschutzrechtlich relevanten Themen, sofern sie Einfluss haben auf die Arbeit in den Einrichtungen und Diensten.
- Er sorgt dafür, dass Verfahrensanweisungen und Anordnungen eingehalten werden.
- Und schließlich dient er natürlich als Ansprechpartner für die Mitarbeiter zu allen datenschutzrechtlichen Problemen und Fragestellungen.

Abb. 6: Die Schweigepflicht

Eine besondere Rolle im Datenschutz spielt die **Schweigepflicht** (Abb. 6). Sie unterliegt neben den datenschutzrechtlichen auch straf- und arbeitsrechtlichen Gesetzen und Verordnungen. Damit sind Mitarbeiter zur Verschwiegenheit gegenüber Dritten über arbeitsrelevante und vertrauenswürdige Informationen verpflichtet. Diese umfassen alle Lebenshintergründe, die der Betroffene über sich erzählt oder offenbart, also alle persönlichen, beruflichen und wirtschaftlichen Verhältnisse. Selbst die Information, dass der Betroffene „Kunde" einer Einrichtung oder eines Dienstes ist, fällt unter die Schweigepflicht.

Im Organisationshandbuch einer Einrichtung könnte also stehen: „Jedwede Information über Klienten, Hilfeempfänger oder Dritte, die zu uns eine Rechtsbeziehung unterhalten, unterliegen neben den staatlichen und kirchlichen Datenschutzgesetzen auch der Verschwiegenheit innerhalb unserer Einrichtung."

Die Vorgaben zur Schweigepflicht gehen recht weit und beeinflussen maßgeblich, wie wir datenschutzrechtlich konforme vertrauliche Gespräche und Telefonate führen und wie wir mit E-Mails und dem Internet umgehen.

Abb. 7: Vertrauliche Gespräche führen

Wie sollten Sie **vertrauliche Gespräche** mit Kunden, Klienten, Bewohnern, Patienten, Angehörigen und auch mit Kollegen führen (Abb. 7)? Zunächst achten Sie unbedingt darauf, öffentliche Räume zu meiden. Dritten sollte nicht die Möglichkeit eingeräumt werden, sensible Gespräche mit zu lauschen. Bitten Sie also die Betroffenen in einen geschlossenen Raum, in dem Sie ungestört kommunizieren können.

Weisen Sie bei Gesprächsanfragen Ihre Gesprächspartner darauf hin, dass die Flure und Treppenhäuser Ihrer Einrichtung keine Orte für vertrauliche Gespräche sind.

Häufig geraten Sie in Situationen, in denen Sie während eines vertraulichen Gespräches gestört werden – sei es durch eingehende Telefonate oder durch Dritte. Versuchen Sie diese Störungen weitestgehend zu verhindern. Falls dies nicht möglich ist, vermeiden Sie es unbedingt, datenschutzrelevante Informationen im Dreiecksverhältnis zu besprechen. Bieten Sie bei Telefonaten den eigenen Rückruf an, vereinbaren Sie verbindliche Termine oder bitten Ihren Gesprächspartner kurz heraus.

Und lassen Sie bitte keine Gesprächsunterlagen und –ergebnisse offen und für alle sichtbar auf Ihrem Schreibtisch liegen, wenn Sie auch nur kurz den Raum verlassen.

Abb. 8: So telefonieren Sie richtig

Was für persönliche Gespräche gilt, das hat auch bei Telefonaten grundsätzliche Bedeutung. Auch ein **datenschutzkonformes Telefonieren** will gelernt sein (Abb. 8).

⁞ Falls Sie meinen, Sie könnten mal eben während Ihrer gerade ausgeübten Tätigkeit nebenher ein paar (möglicherweise sogar vertrauliche) Telefonate führen, so irren Sie sich. Meistens sind Menschen nicht wirklich in der Lage, mehrere Dinge gleichzeitig zu tun. Multitasking funktioniert in den meisten Fällen also nicht. Konzentrieren Sie sich daher bitte auf einen einzigen Vorgang.

⁞ Kennen Sie eigentlich Ihren Gesprächspartner, mit dem Sie gerade das Telefonat führen? Wenn nicht, sollten Sie sich nicht dazu verleiten lassen, persönliche oder sicherheitsrelevante Daten am Telefon herauszugeben. Rufen Sie stattdessen zurück oder recherchieren Sie zuvor Ansprechpartner und Telefonnummer.

⁞ Vermeiden Sie bei Telefonaten, dass Dritte mithören können. Suchen Sie einen ruhigen Ort auf, an dem Sie ungestört telefonieren können.

⁞ Verzichten Sie gerade am Telefon auf das Preisgeben allzu vieler Informationen. Beschränken Sie sich stattdessen auf die allernötigsten Daten.

⁞ Bei Festnetzanschlüssen werden viele dieser Bedingungen allein schon aufgrund der räumlichen Beschränkungen mehr oder weniger erfüllt. Besonders die Nutzung von Smartphones für dienstliche Angelegenheiten sollte aber mit Bedacht erfolgen. Hier gilt es darauf zu achten, dass sensible Daten nicht auf dem Smartphone gespeichert werden. Bei Verlust des Gerätes könnten diese Informationen ansonsten in unbefugte Hände geraten. In diesem Zusammenhang spielt auch die Wahl und Anwendung geschützter PIN-Nummern eine Rolle. Falls Sie sich Ihre PIN-Nummer notieren müssen, so bewahren Sie diese unter keinen Umständen in unmittelbarer Nähe Ihres Smartphones auf.

Abb. 9: Was ist am Arbeitsplatz zu beachten?

Was sollten Sie am Arbeitsplatz unter datenschutzrechtlichen Aspekten beachten (Abb. 9)? Vieles hängt damit zusammen, dass Ihr Büro oder Arbeitsplatz nicht von unbefugten Dritten ohne Ihr Beisein betreten werden sollte. Schließen Sie also Ihr Büro oder den Besprechungsraum grundsätzlich ab, wenn Sie ihn als letzte Person verlassen, sofern sich vertrauliche Unterlagen darin befinden, die zuvor nicht in einem Schrank oder der Schublade verschlossen wurden. Verwahren Sie die Schlüssel an einem sicheren Ort.

Achten Sie darauf, keine unbefugten Personen an Ihren Schreibtisch oder Computer zu lassen. Verwenden Sie unterschiedliche Passwörter, wenn sich mehrere Mitarbeiter einen PC teilen.

Und transportieren Sie Unterlagen stets in undurchsichtigen Schutzhüllen (also Mappen oder Ordner) und schützen Sie diese somit vor dem Zugriff unbefugter Personen.

Abb. 10: Ihr gefährlichstes Möbelstück…

Was ist (zumindest aus datenschutzrechtlichen Gründen) eigentlich das gefährlichste Möbelstück in Ihrem Büro oder an Ihrem Arbeitsplatz? Wahrscheinlich haben Sie sich darüber noch keine Gedanken gemacht, aber die größten Gefahren lauern im Papierkorb (Abb. 10). Fehlt ein Aktenvernichter oder eine besondere Papiertonne für Datenmüll, so wandert eine Vielzahl an Unterlagen (auch mit sensiblen Daten) einfach in den allgemeinen Papierkorb. Man hat schon Berge an Personal- und Bewerbungsunterlagen später säuberlich gestapelt in Papiercontainern wiedergefunden.

Achten Sie also darauf, keine Unterlagen mit vertraulichen Daten in den Papierkorb zu werfen. Dies gilt nicht nur für den eigenen Arbeitsplatz, sondern auch für Papierkörbe neben Zentraldruckern und Kopierern. Natürlich erstreckt sich dies auch auf CDs, DVDs und USB-Sticks mit personenbezogenen Daten.

Abb. 11: Umgang mit E-Mails

Apropos elektronische Daten. Heutzutage wird ein Großteil an relevanten Daten EDV-mäßig erfasst. Auch der Transport von Daten wird mittlerweile weitgehend über E-Mails vorgenommen. Doch gerade der sorglose **Umgang mit E-Mails** könnte datenschutzrechtlich gravierende Folgen nach sich ziehen (Abb. 11).

Wie schnell werden mal eben nebenbei Mails an einzelne Personen oder gar ganze Verteiler verschickt? Sie sollten dabei einige Dinge beachten:

⁞ Sehen Sie wenn möglich von offenen E-Mail-Verteilern ab, vor allem dann, wenn es sich um das Versenden sensibler Daten handelt. Ihre Verteiler sollten Sie zumindest genau im Blick behalten und sich immer bewusst sein, welche Personen genau dahinterstecken.

⁞ Wie gehen Sie mit E-Mails in Urlaubszeiten um? Hier bietet sich entweder eine automatische Antwort-Mail oder eine direkte Weiterleitung zu Ihrer Urlaubsvertretung oder zu einem Kollegen an. Achten Sie darauf, dass diese Person die datenschutzrechtlich gleichen Befugnisse hat wie Sie selbst.

⁞ Achten Sie im Mail-Eingang auf den Versender der Nachricht. E-Mails können Viren, Trojaner und Malware einschleppen. Öffnen Sie nur Mails bzw. Mailanhänge, denen Sie vertrauen.

Am besten verzichten Sie (so gut es geht) auf das Versenden von sensiblen Daten per E-Mail.

Sehen wir uns schließlich noch eine mögliche Passage aus einem Organisationshandbuch einer Einrichtung zur E-Mail-Nutzung an: „Die private Nutzung der dienstlichen E-Mail-Adresse ist nicht zulässig. Der Vorgesetzte hat jederzeit ein Zugriffsrecht auf das E-Mail-Konto. Der Vorgesetzte kann die Rechte an einem E-Mail-Konto jederzeit an einen anderen Mitarbeiter delegieren."

Der E-Mail-Verkehr ist allerdings nur *ein* (wenngleich wichtiger) Bestandteil des Themas Datenschutz bei der Nutzung von Computern und EDV-Anlagen. Was sollten Sie darüber hinaus noch für die Arbeit an und mit Computern wissen (Abb. 12)?

Abb. 12: Der richtige Umgang mit dem Computer

⁞ Stellen Sie den Monitor Ihres Computers so auf, dass unbefugte Personen ihn nicht einsehen können.

⁞ Verwenden Sie einen passwortgeschützten Bildschirmschoner, damit Ihre Arbeit auch in kurzen Abwesenheitszeiten nicht beobachtet werden kann.

⁞ Ihr Computerzugang sollte nur Ihnen selbst über ein Passwort möglich sein. Im Organisationshandbuch könnte stehen: „Nutzer erhalten Zugang zu den EDV-Systemen, die für die Erfüllung notwendig bzw. sinnvoll sind. Der Nutzer ist für die Geheimhaltung und regelmäßige Änderung seines Passwortes sowie der Geheimhaltung seiner Zugangsdaten selbstständig verantwortlich. Nutzer von EDV-Systemen dürfen sich nicht unberechtigten Zugang zu

den Daten anderer, auch nicht anderer Dienste, verschaffen, diese weitergeben oder manipulieren."

⁞ Und schließlich überlegen Sie sich sehr gut, an welchen Ort und auf welche Medien Sie sensible Daten speichern. Beachten Sie unbedingt die Vorschriften zum Datenschutz und schützen Sie Ihre Daten vor Zerstörung und Manipulation.

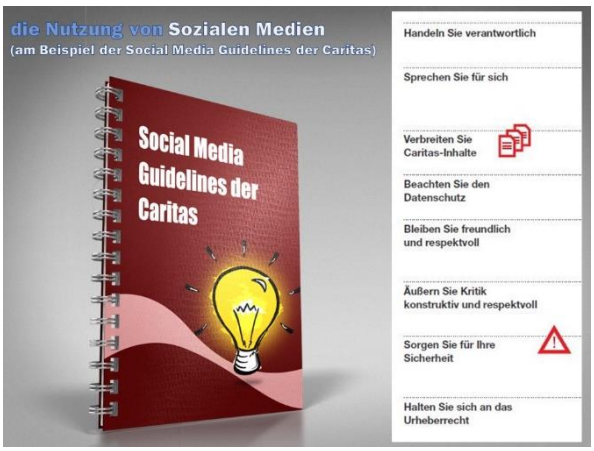

Abb. 13: Die Nutzung von Sozialen Medien

Bleiben noch die **sozialen Medien**. Facebook, twitter & co nehmen heute eine wichtige Funktion in der zwischenmenschlichen Kommunikation wahr und sind aus unserem Lebensalltag kaum mehr wegzudenken (Abb. 13).

⁞ Als oberstes Prinzip gilt jedoch: Trennen Sie unbedingt die private von der beruflichen Nutzung von sozialen Netzwerken. Klare Anweisungen könnten auch im Organisationshandbuch einer Einrichtung enthalten sein: „Den Mitarbeitern ist es untersagt, berufliche Angelegenheiten über die sozialen Medien wie Twitter, Facebook etc. zu kommunizieren." Das bedeutet aber nicht, dass Sie als Privatperson nicht Stellung nehmen dürfen zu gesellschaftspolitischen Themen und zu inhaltlichen Aspekten Ihrer Arbeit. Ganz im Gegenteil animieren z.B. Spitzenverbände der Freien Wohlfahrtspflege wie etwa der Deutsche Caritasverband e.V. seine Mitglieder und all seine Beschäftigten zu einem verantwortungsvollen Umgang mit sozialen Medien.

⁞ Gemäß den **Social Media Guidelines** – hier am Beispiel der Caritas - soll mit sozialen Medien Menschen direkter und schneller geholfen werden, indem Online-Beratungen und Dienste vor Ort zugänglich gemacht werden. Vor allem junge Leute sollen mit den Ideen, Angeboten und Aktionen Ihres Unternehmens in Kontakt gebracht werden und die Vernetzung mit Personen, die spenden, stiften oder sich engagieren wollen, soll intensiviert werden. Durch den Kontakt mit anderen Menschen und deren Feedback sollen Angebote optimiert werden. Positionen und Aktionen Ihrer Arbeit sollen in die sozialpolitische Debatte im Netz eingebracht werden, so dass Ihre Beiträge in sozialen Medien dazu beitragen, einen Knoten im Netzwerk vieler Menschen zu bilden, die an sozialen Themen interessiert sind und die als Multiplikatoren von Ideen gewonnen werden.

⁞ Handeln Sie verantwortlich. Unsere glaubwürdigsten Botschafter sind Sie: die Mitarbeiterinnen und Mitarbeiter, die Auszubildenden und die vielen Freiwilligen und Ehrenamtlichen. Durch Ihren Einsatz geben Sie Ihrer Arbeit vor Ort ein Gesicht – tun Sie dies gerne auch in Ihren sozialen Netzwerken.

⁞ Sprechen Sie für sich. Entscheiden Sie selbst, ob Sie in sozialen Netzwerken angeben, dass Sie in Ihrer Einrichtung arbeiten. Für Ihre Inhalte sind Sie selbst verantwortlich. Machen Sie deutlich, in welcher Funktion Sie beschäftigt sind. Offizielle Statements geben nur der Vorstand, die Geschäftsführung oder dazu beauftragte Personen. Sie äußern Ihre persönliche Meinung und bringen dabei Ihr fachliches Know-how ein.

⁞ Verbreiten Sie wichtige Inhalte. Werden Sie Botschafterin oder Botschafter Ihres Unternehmens, indem Sie interessante Inhalte und Angebote Ihrer Einrichtung verlinken, kommentieren und mit anderen teilen.

⁞ Beachten Sie den Datenschutz. Machen Sie keine Aussagen über Klienten, Patienten, Kunden, Spendern Kollegen oder Geschäftspartner in sozialen Medien.

⁞ Bleiben Sie freundlich und respektvoll. Der Dialog in sozialen Netzwerken ist zum Teil hitzig, manchmal unfair und beleidigend. Bleiben Sie sachlich und halten Sie sich an die Fakten.

⋮ Verweisen Sie im Zweifelsfall auf die Sprecherinnen und Sprecher Ihres Verbandes oder Ihrer Einrichtung.

⋮ Äußern Sie Kritik konstruktiv und respektvoll. Soziale Netzwerke ermöglichen offene Diskussionen. Sie sind aber der falsche Ort, um Probleme am Arbeitsplatz oder mit einzelnen Personen zu diskutieren, dies sollte eher im direkten Gespräch geschehen.

⋮ Sorgen Sie für Ihre Sicherheit. Passen Sie auf allen Plattformen Ihre Einstellungen zur Privatsphäre an. Geben Sie Ihre Zugangsdaten nicht an Dritte weiter und lesen Sie sich jede Äußerung noch einmal durch, bevor Sie sie veröffentlichen. Sprechen Sie sich im Zweifel mit einer Kollegin oder einem Kollegen ab.

⋮ Und halten Sie sich an das Urheberrecht. Veröffentlichen Sie Fotos, Filme oder Audiomaterial nur, wenn Sie dazu berechtigt sind. Nennen Sie Ihre Quellen und kennzeichnen Sie Zitate.

Abb. 14: Urheberrecht und Recht am eigenen Bild

Immer wenn Sie Informationen oder eigene Beiträge veröffentlichen möchten, sei es im Internet oder in Form von Flyern, Broschüren, Programmheften, Zeitungsartikeln oder Hauszeitungen, so sehen Sie sich mit Fragen des **Urheberrechts** konfrontiert (Abb. 14). Als Urheberrecht wird das Recht auf den Schutz geistigen Eigentums in materieller und ideeller Hinsicht bezeichnet. Verwenden Sie also Texte oder Bildmaterial fremder Personen, z.B. nach einer Internetrecherche, so müssen Sie zunächst feststellen, wem die Urheberrechte an diesem Material zustehen. Nur in seltenen Fällen können die gefundenen Materialien frei und kostenlos für eigene Zwecke verwendet werden. Nehmen Sie im Zweifel immer Kontakt zum Urheber auf.

In eine ganz ähnliche Richtung bewegt sich das **Recht am eigenen Bild**. Es beinhaltet, dass jeder Mensch grundsätzlich selbst darüber bestimmen darf, in welchem Zusammenhang (und ob überhaupt) Bilder von ihm veröffentlicht werden und falls ja, für welche Zwecke und in welcher Form. Vor allem unsere Pressearbeit wird begleitet von einer Vielzahl an Fotos, auf denen eine oder mehrere Personen abgebildet sind. Sie sollten grundsätzlich davon ausgehen, dass Sie die ausdrückliche und schriftliche Einwilligung jeder abgebildeten Person zur Veröffentlichung einholen müssen.

Sie haben festgestellt, dass das Thema Datenschutz in sozialen Diensten und Einrichtungen ein sehr weites Gebiet ist. Bitte beachten Sie die Vorgaben in Ihrer täglichen Arbeit und weisen Sie auf Missstände hin.