

Datenschutz und wie Sie rechtssicher damit umgehen

Datenschutz ist ein Thema, mit dem sich Kindertageseinrichtungen weniger beschäftigen. Dies liegt jedoch nicht daran, dass es an Brisanz und Aktualität fehlt, sondern daran, dass Grundsätzliches zum Datenschutz **in den Einrichtungen weniger bekannt** ist.

Schützenswerte Daten in Ihrer Kindertageseinrichtung

Der **Datenschutz bezieht sich auf die personenbezogenen Daten** in Ihrer Kindertageseinrichtung. Personenbezogene Daten sind alle Daten, die eine Person beschreiben oder Aussagen zu dieser Person machen. Der Datenschutz in Kindertageseinrichtungen bezieht sich auf Eltern, Kinder, Mitarbeiterinnen und Vernetzungspartner, mit denen Sie zusammenarbeiten. Zu folgenden Personengruppen speichern Sie Daten in Ihrer Kindertageseinrichtung:

Kundendaten: Alle **Daten**, die Sie **zu Eltern und Kindern** in der Einrichtung festhalten. Dies sind beispielsweise Daten, die auf der Karteikarte notiert sind, wie Adressen, Telefonnummern, Sorgerechtsregelungen, Informationen zum Kind und zur Familie. Auch Bankverbindungen der Eltern, die Sie für das Einzugsverfahren der Elternbeiträge benötigen, zählen zu Ihren Kundendaten.

Vernetzungsdaten: Auch **Daten**, die **durch Gespräche** und Informationen **mit** Ihren so genannten **Vernetzungspartnern** entstanden sind, halten Sie in Ihrer Einrichtung fest. Diese Daten sind z. B. Informationen des Allgemeinen Sozialen Dienstes über eine mögliche Gefährdung des Kindeswohls in der Familie oder die Nachricht der Lehrerin, die den plötzlichen Leistungsabfall des Kindes mit der anstehenden Scheidung der Eltern begründet.

Mitarbeiterdaten: Von Ihren Mitarbeiterinnen speichern Sie üblicherweise **Adressdaten und alle Daten**, die Sie **zur Personalverwaltung** benötigen, wie beispielsweise das Geburtsdatum, berufliche Bewährungszeiten, Eintrittsdatum in die Einrichtung, arbeitsvertragliche Vereinbarungen und Kontodaten, die relevant für die Lohn- und Gehaltsabrechnung sind. **Lieferantendaten:** Von allen **Firmen, die Sie beliefern**, wie Lebensmittellieferanten oder Materialausstatter, verwalten Sie Daten, beispielsweise Bestelllisten, Rechnungen, Kontoauszüge und Kontonummern der Lieferanten.

Grundsätze für Ihren Umgang mit personenbezogenen Daten

1. Erheben Sie grundsätzlich nur personenbezogene Daten, indem Sie die jeweilige Person darüber in Kenntnis setzen. **Informieren Sie die Eltern** oder Ihre Mitarbeiterinnen darüber, **wenn Sie personenbezogene Daten über sie festhalten**. Dabei ist es hilfreich, wenn Sie erklären, zu welchem Zweck Sie diese Daten benötigen.

2. Erfassen Sie nur solche Daten, die tatsächlich für Ihre Arbeit nötig sind. **Überlegen Sie** grundsätzlich, **welche Daten Sie benötigen**. Verzichten Sie auf alle Daten, die für Ihre Arbeit nicht relevant sind. So ist es beispielsweise völlig legitim, die Adresse und Telefonnummer der Eltern zu speichern, für den Fall, dass Sie die Eltern schriftlich oder telefonisch informieren müssen. Die Kontonummer der Eltern brauchen Sie jedoch nicht, wenn Sie wissen, dass das Jugendamt den Erziehungsbeitrag für deren Kind übernehmen wird.

3. **Nutzen Sie** die personenbezogenen **Daten nur zu dem Zweck**, zu dem Sie sie erhoben haben. Wenn Sie beispielsweise das Einkommen der Eltern ermitteln müssen, weil der Erziehungsbeitrag Ihrer Einrichtung nach den elterlichen Einkünften gestaffelt wird, dient diese Datenerhebung einem legitimen Zweck. Diesen würden Sie jedoch verfremden, wenn Sie über die Höhe der Einkommensverhältnisse aller Eltern eine Statistik anfertigen und diese veröffentlichen würden.

4. **Treffen Sie** organisatorische **Maßnahmen, die einen Missbrauch** der Daten **verhindern**. Je nachdem, wie Sie die Daten in Ihrer Einrichtung speichern oder aufbewahren, sollten Sie geeignete Vorkehrungen treffen. Sind die personenbezogenen Daten in Akten abgelegt, sollten Sie diese wegschließen und den Schlüssel so aufbewahren, dass keine unbefugten Dritten Zugang zum Schlüssel haben. Sichern Sie Ihre EDV mit einem Passwort, wenn die personenbezogenen Daten auf Ihrem PC gespeichert sind. Zugang zu den Karteikarten der Kinder haben beispielsweise alle Erzieherinnen, während nur der Träger und Sie als Leiterin Zugriff auf die Duplikate der Gehaltsabrechnungen haben sollten.

5. **Löschen** oder vernichten **Sie** die personenbezogenen **Daten**, sobald Sie dem Zweck nicht mehr dienen, für den Sie sie erhoben haben. Wenn Eltern beispielsweise keine Kinder mehr in Ihrer Einrichtung haben oder Ihre Mitarbeiterinnen nicht mehr bei Ihnen arbeiten, müssen Sie die personenbezogenen Daten vernichten. Zur Vernichtung sollten Sie die Daten gänzlich unkenntlich machen, z. B. indem Sie sie durch einen Reißwolf schicken.

Teilen Sie die Daten in Kategorien auf

Gehen Sie generell mit allen **Daten**, die Sie in Ihrer Kindertageseinrichtung verwalten oder aufbewahren, sensibel und behutsam um. Auf der rechtlich sicheren Seite bewegen Sie sich, wenn Sie diese Daten zusätzlich **in** unterschiedliche **Schutzkategorien einstufen**.

Kategorie 1: Nicht besonders schützenswerte Daten

In diese 1. Kategorie fallen **Daten**, die Sie zwar vorliegen haben, die jedoch **nicht besonders schützenswert** sind. Diese Daten können frei zugänglich sein, ohne dass beispielsweise Eltern, die Einsicht nehmen wollen, ein berechtigtes Interesse belegen müssen.

Zu den Daten, die in die 1. Kategorie fallen, gehören z. B.:

- Bestelllisten aller Art, in die die Eltern sich freiwillig eintragen, etwa für Fotos oder Bastelmaterial.
- Jegliche Unterschriftslisten, mit denen die Eltern ihre Bereitschaft bekunden, z. B. dass ihr Kind am Ausflug teilnimmt, dass sie etwas zum gemeinsamen Frühstück beisteuern oder dass sie beim Basar mithelfen.
- Mitgliedsverzeichnisse, z. B. des Vorstands oder des Elternbeirats, die in der Einrichtung aushängen und den Eltern die einzelnen Mitglieder kenntlich machen.

Tipp für Ihre Praxis: **Sammeln Sie** schriftlich **alle Daten**, die in die 1. Kategorie der nicht besonders schutzwürdigen Daten fallen. **Ordnen Sie** diese **nach dem Alphabet**, dann genügt ein Blick in Ihr Abc-Register, wenn Sie sich nicht sicher sind, ob neu anfallende Daten der 1. Kategorie angehören.

Kategorie 2: Daten, zu deren Erhebung Sie das Einverständnis brauchen

Der 2. Kategorie gehören **personenbezogene Daten** an, **die** zwar keinen Missbrauch durch Dritte vermuten lassen, deren Kenntnisnahme jedoch das **Einverständnis des Dateninhabers** – also beispielsweise der Eltern oder der Mitarbeiterinnen – **voraussetzt**.

Daten der 2. Kategorie sind z. B.:

- Persönliche Daten von Kindern, Eltern oder Personal
- Adressdaten
- Telefonnummern
- Informationen zum Familienstand
- Aussagen über die berufliche Tätigkeit
- Konfession
- Aussagen über Gesundheitszustand und Allergien
- Zugehörigkeit zur Krankenkasse

Tipp für Ihre Praxis: Beachten Sie, dass bereits die Bitte einer Mutter um die Telefonnummer eines Kindes, das sie zum Geburtstag ihres Kindes einladen möchte, in diese 2. Kategorie fällt. Sie dürfen die erbetene **Telefonnummer nur mit** dem ausdrücklichen **Einverständnis der Eltern** des Kindes **weiterreichen**.

Kategorie 3: Besonders schützenswerte Daten

Daten der 3. Kategorie sind **besonders schutzwürdig**. Dazu müssen Sie alle Daten rechnen, deren **unbefugte Einsicht** durch Dritte **zu Missbrauch führen könnte**. Dies betrifft vor allem das Ansehen und die gesellschaftliche Stellung der Personen oder deren wirtschaftliche Verhältnisse.

Solche Daten, die der 3. Kategorie angehören, sind beispielsweise:

- Auskünfte über Einkommen
- Daten von Sozialleistungen
- Bankverbindung
- Auskünfte über Familienmitglieder, beispielsweise Vorstrafen des Vaters oder im Heim lebende Kinder der Mutter
- Informationen über innerfamiliäre Verhältnisse, wie z. B. Scheidungsverfahren, Sorgerechtsstreitigkeiten, Adoptionswünsche
- Interna über personelle Angelegenheiten in der Einrichtung, etwa Abmahnungen oder Kündigungen von Mitarbeiterinnen
- Dokumente von Mitarbeitergesprächen
- Aufzeichnungen, Dokumente oder Protokolle über kindliche Entwicklungs- oder Verhaltensauffälligkeiten

Tipp für Ihre Praxis: Halten Sie alle **Unterlagen**, die in die **3. Kategorie** fallen, stets in Ihrer Einrichtung **unter Verschluss**. Sowohl Mitarbeiterinnendaten der Personalverwaltung als auch Kinder- und Elternakten müssen Sie in einem abgeschlossenen Schrank verwahren, zu dem nur Sie und der Träger Zugang haben. Kennzeichnen Sie solche Ordner beispielsweise mit einem roten Orderrücken. Schützen Sie diese Daten, die Sie im PC der Einrichtung verwalten, durch ein persönliches Kennwort.

Teilen Sie die Daten, die in Ihrer Einrichtung anfallen, in die 3 Schutzkategorien ein. So wissen Sie jederzeit, wie wichtig der Schutz dieser Daten und Unterlagen ist. Damit unterläuft Ihnen kein Fehler beim Datenschutz.