anthroSocial
begegnen begleiten befähigen

Merkblatt

Datenschutzrelevante Aspekte für Meldestellen in Einrichtungen der Behindertenhilfe

Dieses Merkblatt richtet sich an Fachpersonen, die in Einrichtungen der Behindertenhilfe mit der Leitung oder Mitarbeit in Präventions- und Meldestellen betraut sind. Es fasst zentrale datenschutzrechtliche Aspekte zusammen, die im Umgang mit Meldungen von Grenzverletzungen und Gewalt zu beachten sind. Datenschutz bedeutet dabei nicht in erster Linie den Schutz der Daten selbst, sondern der Schutz der betroffenen Person vor einem Missbrauch oder einer nicht gerechtfertigten Nutzung ihrer personenbezogenen Informationen. Als personenbezogene Daten gelten alle Informationen, die sich einer bestimmten oder zumindest identifizierbaren Person zuordnen lassen. Der Datenschutz verfolgt das Ziel, die Persönlichkeits- und Grundrechte jener Menschen zu wahren, deren Daten verarbeitet werden (vgl. AvenirSocial 2023).

Die Hinweise in diesem Merkblatt basieren auf der Verbandsbroschüre von AvenirSocial zu «Datenschutz in der Sozialen Arbeit» (2023), den Vorgaben des bundesrechtlichen Datenschutzgesetzes (DSG), einschlägigen kantonalen Regelungen sowie Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Die Hinweise wurden juristisch von Prof. Peter Mösch lic.iur. LL.M. überprüft. Sie sollen Fachpersonen eine praxisnahe Orientierung bieten, um Meldestellen datenschutzkonform und gleichzeitig wirksam zu gestalten. Wichtig anzumerken ist jedoch, dass kantonale und kommunale öffentliche Organe den kantonalen Datenschutzgesetzen unterworfen sind. Dazu gehören auch Institutionen, die öffentliche/gesetzliche Aufgaben nach kantonalem Recht wahrnehmen, auch wenn sie eine private Trägerschaft aufweisen. Es ist deshalb im Zweifel notwendig, die nachfolgenden allgemeinen Richtlinien mit den kantonalen Datenschutzbehörden (Adressen siehe Link am Ende des Dokuments) zu verifizieren. Diese stehen, wie auch allfällige Datenschutzbeauftragte der Institution, für Fragen zur Verfügung.

1. Aufbewahrung und Archivierung

- Die gesetzliche Aufbewahrungsfrist richtet sich nach den kantonalen Vorgaben. Eine einrichtungsinterne Regelung sollte dies präzisieren.
- Vorfallmeldungen und damit verbundene Unterlagen (u.a. Dokumentation zur Bearbeitung der Vorfallmeldung) sollten in der Regel mindestens 10 Jahre aufbewahrt werden. Kantonale Vorgaben können längere Fristen vorsehen (z. B. 80 Jahre im Kanton Bern für Betreuungsakten).
- Eine längere Aufbewahrung kann im Sinne des biografischen Rückbezugs gerechtfertigt sein – dies sollte jedoch sorgfältig dokumentiert und begründet werden.
- Bei der Auflösung einer Institution sollte vorgängig eine Regelung zur Archivierung sensibler Daten getroffen werden, z. B. durch Übergabe an eine Nachfolgeinstitution oder ein staatliches Archiv.

2. Zugriff und Einsichtnahme

- Zugriff auf sensible Daten, wie z.B. Vorfallmeldungen sollten nur klar definierte Personen mit entsprechendem Rollenbezug erhalten. Dies ist in einem Berechtigungskonzept festzuhalten.
- Sensible Daten, wie z. B. Vorfallmeldungen, müssen sowohl digital als auch physisch gesichert aufbewahrt werden. Digital bedeutet, dass entsprechende Ordner auf dem Server nur über passwortgeschützte Zugänge erreichbar sind und mit individuellen Benutzerrechten versehen werden. Analoge Unterlagen sind in abschliessbaren Schränken aufzubewahren. Den Schlüssel hierzu haben nur dafür berechtigte und definierte Personen.
- Sind die Daten auf Servern gespeichert, so ist mittels angemessener technischer Vorkehren zu sichern, dass kein Zugriff für unbefugte Dritte möglich ist (Schutz vor Cyberangriffen etc.)
- Zugriffe auf sensible Daten, z.B. Vorfallmeldungen sind technisch zu protokollieren. Es ist regelmässig zu prüfen, ob die erfolgten Einsichtnahmen begründet sind. Evt. sind entsprechende Vorgaben anzupassen, oder bei unbefugtem Zugriff Massnahmen zu ergreifen und zu dokumentieren. Im Zweifel hat eine Meldung an den eidgenössischen bzw. kantonalen Datenschutzbeauftragten zu erfolgen.
- Klient:innen sowie deren gesetzliche Vertretungen (Vertretungsbeistandschaft mit einem entsprechenden Mandat oder umfassende Beistandschaft) haben grundsätzlich das Recht auf Einsicht in ihre personenbezogenen Daten. Dabei muss der Schutz Dritter (z. B. namentlich genannter Personen in Vorfallmeldungen) bspw. durch Einschwärzung des Namens und weiterer persönlicher Informationen, gewährleistet bleiben.
- Bei Herausgabe von Unterlagen an Klient:innen ist eine fachliche Begleitung bei der Einsichtnahme sinnvoll, um Missverständnisse zu vermeiden und eine unnötige Belastung zu vermeiden.

3. Weitergabe von Daten an Dritte

- Die Weitergabe sensibler Daten, z.B. Vorfallmeldung an Dritte bedarf entweder einer gesetzlichen Grundlage oder einer informierten Einwilligung der betroffenen Person bzw. bei diesbezüglicher Urteilsunfähigkeit der gesetzlichen Vertretung.
- Bei gesetzlichen Vertreter:innen oder Angehörigen ist zu prüfen, ob die Zustimmung der urteilsfähigen betroffenen Person vorliegt. Liegt keine Urteilsfähigkeit der betroffenen Person vor ist eine Weitergabe dann zulässig, wenn sie dem mutmasslichen Willen der betroffenen Person entspricht. Überdies muss immer das Wohl der schutzbedürftigen Person beachtet werden.
- Vor der Weitergabe an Dritte müssen Betroffene bzw. bei diesbezüglicher Urteilsunfähigkeit die gesetzliche Vertretung grundsätzlich informiert werden. Ausser es besteht eine rechtliche Verpflichtung zur Meldung (z. B. bei Gefährdungsmeldungen).
- Daten Dritter, die z.B. in einer Vorfallmeldung erwähnt werden (z. B. weitere Beteiligte, Zeug:innen), sind besonders zu schützen z.B. durch Einschwärzen. Sie sind nur bei zwingendem überwiegendem Interesse (z.B. aufgrund ausdrücklicher gesetzlicher Grundlage) weiterzugeben.

4. Digitalisierung und sichere Kommunikation

- Für digitale Erfassung und Übermittlung sensibler Daten sind verschlüsselte Systeme zu verwenden (z. B. HIN, IncaMail, sichere Serverlösungen). Office-Mail genügt den Anforderungen in der Regel nicht.
- Systeme wie RedLine, Socialweb oder M365 können genutzt werden, sofern deren Datenschutzkonfigurationen korrekt eingestellt sind und der Zugriff kontrolliert wird.

- Empfänger:innen sensibler Daten sollten vorgängig schriftlich bestätigen, dass sie die Informationen vertraulich und datenschutzkonform behandeln.
- Die Speicherung auf privaten Geräten oder offenen Servern ist zu vermeiden.

5. Dokumentation und Bearbeitungsprozesse

- Die Bearbeitung eines Vorfalls sollte nachvollziehbar dokumentiert werden: Zeitpunkt, beteiligte Personen, Einschätzung, Massnahmen, Verlauf.
- Je nach Schweregrad (z. B. gemäss Einstufungsraster) kann ein unterschiedlicher Detaillierungsgrad der Dokumentation erforderlich sein.
- Für Bearbeitungsunterlagen gelten grundsätzlich dieselben Aufbewahrungsfristen wie für Vorfallmeldungen.

6. Schweigepflicht und Einwilligung

- Eine schriftliche Entbindung von der Schweigepflicht durch die betroffene Person oder deren gesetzliche Vertretung ist bei Datenweitergabe an z. B. Opferhilfe, Polizei oder Justiz empfehlenswert.

7. Umgang mit besonderen Situationen

- Fotos von Verletzungen dürfen von Betreuungspersonen nur bei dokumentiertem Verdacht und mit grösster Zurückhaltung gemacht werden, sofern keine andere Beweissicherung möglich ist. Eine ärztliche Einschätzung ist vorzuziehen.
- Bei Wechsel der Einrichtung dürfen Informationen über schwere Vorfälle nur mit informierter Einwilligung der betroffenen Klientin/des betroffenen Klienten resp. deren gesetzlichen Vertretung oder bei erheblicher Gefährdung weitergegeben werden.
- Bei internen Vorfällen (z. B. Entlassung nach Gewaltanwendung) ist eine transparente, aber datensensible Kommunikation notwendig.
- Daten wie die Anzahl Vorfallmeldungen dürfen nur dann im Rahmen von klientelspezifischen Entwicklungsplanungen verwendet werden, wenn dies datenschutzkonform erfolgt und ein Bezug zur Verbesserung des Unterstützungsangebots gegeben ist.

Weiterführende Hinweise und relevante Links

- Avenir Social (2023): Datenschutz in der Sozialen Arbeit: **Datenschutz-i-d-SA_180123.pdf**
- Datenschutzgesetz (DSG) und entsprechende Verordnungen: **Rechtsgrundlagen Datenschutz**
- Verzeichnis aller kantonaler Datenschutzbeauftragten: **Organisation (DE) – privatim**
- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter: **Willkommen beim EDÖB**