Datenschutz im CM-Prozess - Voraussetzungen

- Die erfolgreiche Durchführung eines Case Management-Verfahrens setzt das Vertrauen der Klientinnen und Klienten voraus. Ein solches Vertrauen ist nur denkbar, wenn betreffend der Verwendung der Personendaten vollständige Klarheit und Transparenz herrschen. Den datenschutzrechtlichen Grundsätzen ist auch deshalb die erforderliche Seriosität beizumessen.
- Die Informationen müssen auch im Case Management grundsätzlich immer bei der betroffenen Person selbst beschafft werden.
- Generalvollmachten und Blankovollmachten sind aus datenschutzrechtlicher Sicht unzulässig (Transparenz).

Datenschutz – technische Lösungen für den ersten Schritt

Allgemeiner E-Mail-Austausch

Unsere Expertinnen-/Expertenbefragung zeigte, dass insbesondere im E-Mail-Kontakt unterschätzte Risiken bestehen. E-Mail-Kommunikation ist annähernd mit dem Postkartenversand zu vergleichen.
→ Vertraulichkeit ist nicht gewährleistet!

Einfacher verschlüsselter E-Mail-Austausch

Auf relativ einfache Weise lässt sich der E-Mail-Verkehr sicherer gestalten. In diesem Zusammenhang heisst der Schlüsselbegriff „Verschlüsselung". Folgende Sicherheitsmassnahmen sind einfach zu realisieren.

- Grundsätzlich: **Informationen zur Klientschaft nur codiert** und im Rahmen der datenschutzrechtlichen Grundlagen versenden.
- **Klienteninformationen** nicht direkt ins Mail schreiben. Informationen **gehören in** eine **Datei**, welche **passwortgeschützt und verschlüsselt ist.** Diese verschlüsselte Datei wird versandt. Die meisten Software-Lösungen ermöglichen dies auf einfache Art
  - Z. B. Microsoft Office 2007 für Word, Excel, Power-Point" usw. → unter Hilfe→ Stichwort „Datenschutz" → „Festlegen eines Kennworts zum Öffnen oder Ändern eines Dokuments, einer Arbeitsmappe oder einer Präsentation" gibt es Anleitungen, ebenso bieten dies OpenOffice, OpenCalc usw.)
    Das Kennwort wird z.B. per Telefon oder in separatem Mail an die entsprechende Person weitergegeben.
  - Software, die zum Komprimieren von Dateien eingesetzt wird, bietet ebenfalls Passwortschutz und Verschlüsselung an, beispielsweise 7zip oder WinZip[1].

Aufwändigere und insgesamt sicherere Varianten der Verschlüsselung

- Das sind so genannte asymmetrische Systeme.
  Sie funktionieren, ohne dass zwischen Sender und Empfänger ein Passwort ausgetauscht werden müsste. Zwei Systeme werden heute genutzt, OpenPGP und X.509 (X/MIME).
- Kostenlos erhältlich und im Sozialwesen teilweise bekannt ist GPG4win (www.gpg4win.org).
- Wer sich für diese Sicherheitsstufe interessiert, wird nicht umhin kommen, sich eingehender mit dem Thema Verschlüsselung zu beschäftigen bzw. die zuständige Informatik in den Prozess einzubeziehen. Grundsätzlich empfehlen wir bei technischen Datenschutzaspekten den Einbezug von Informatik-Fachkräften.

Case-Management-Projekt und Datenschutz

- Schon heute muss der Datenschutz im Arbeitsalltag eingehalten werden. Es ist keine Thematik

1 AES256 gilt heute als „sichere" Verschlüsselung. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren verwendet werden. In den USA wird er für staatliche Dokumente der höchsten Geheimhaltungsstufe verwendet.

des Pilotprojektes Case Management in der Sozialberatung. Deshalb wird im Rahmen des Case-Management-Projektes die lückenlose Einhaltung der datenschutzrechtlichen Grundlagen erwartet.

- Eine Verschlüsselungslösung (siehe vorgängige Varianten) ist unerlässlich.
- Es stellt sich auch die Frage, wie die Daten lokal geschützt sind. Auch hier bieten sich die beschriebenen Verschlüsselungslösungen an, wobei zusätzlich auch die Verschlüsselung von (virtuellen) Laufwerken möglich ist, siehe www.truecrypt.org.