Checkliste Datenschutz

1. Vorbereitung

Laden Sie die Datei zur Einwilligungserklärung weiter oben herunter und passen sie diese auf Ihr spezifisches Projekt an. Bspw. ergänzen Sie Projektinformationen, Ziel der Forschung und Adressdaten. Drucken Sie das Dokument zweimal aus, um eines auszuhändigen und eines (unterschrieben) behalten zu können.

2. Verpflichtung auf Datengeheimnis

Alle Personen die an Ihrem Projekt mitarbeiten, bspw. interne MitarbeiterInnen, studentische Hilfskräfte und Studierende etc., müssen auf das Datengeheimnis verpflichtet werden. Ein Muster der unabhängigen Datenschutzbehörden des Bundes und der Länder finden Sie hier.

3. Information

Informieren Sie Ihre InterviewpartnerInnen vorab über die Inhalte der von Ihnen angepassten Einwilligungserklärung: Darüber, dass Sie das Gespräch aufzeichnen, transkribieren und auswerten möchten. Erläutern Sie, für welchen Zweck Ihre Forschung bestimmt ist, wer Zugang zu den Daten hat und wie Sie mit dem Datenschutz umgehen werden. Wir empfehlen bei Bedarf, in Ergänzung zur schriftlichen Einwilligungserklärung, einzelne Passagen mündlich zu erläutern.

4. Einwilligung

Lassen Sie die InterviewpartnerInnen die Einwilligungserklärung unterzeichnen und behalten Sie dieses Dokument. Sind InterviewpartnerInnen unter 16 Jahre alt, ist die Einwilligung von den Eltern zu unterzeichnen (ergänzende Informationen stellt das Bayerische Landesamt für Datenschutzaufsicht hier bereit). Sofern besondere Kategorien personenbezogener Daten betroffen sind, müssen zusätzliche Datenschutzanforderungen beachtet werden (Hinweise der unabhängigen Datenschutzbehörden des Bundes und der Länder finden Sie hier). Händigen Sie den interviewten Personen jeweils eine Kopie der Einwilligungserklärung aus.

Ein Muster einer Einwilligungserklärung – erstellt von unserem Datenschutzbeauftragten finden Sie hier: https://www.audiotranskription.de/qualitative-Interviews-DSGVO-konform-aufnehmen-und-verarbeiten

5. Aufzeichnen, Übertragen und Speichern

Stellen Sie sicher, dass der Speicherort für die personenbezogenen Daten der InterviewpartnerInnen möglichst im Geltungsbereich der DSGVO liegt (Europäische Union - EU oder Europäischer Wirtschaftsraum - EWR). Optimal ist hier das Netzlaufwerk der Hochschule oder lokale Datenträger auf passwortgeschützten Rechnern. Der unverschlüsselte Versand per E-Mail ist für vertrauliche Daten nicht geeignet. Für eine Übermittlung personenbezogener Daten in ein Land außerhalb der EU/des EWR beachten Sie bitte die zusätzlichen Datenschutzanforderungen. Diesbezügliche Hinweise der unabhängigen Datenschutzbehörden des Bundes und der Länder finden Sie hier.

Die Daten müssen schließlich durch technische und organisatorische Maßnahmen insbesondere vor dem unberechtigten Zutritt, Zugang und Zugriff geschützt sein. Das Minimum an Sicherheit sollte ein nicht öffentlich zugänglicher Rechner mit aktuellem und supportfähigem Betriebssystem (kein Windows XP, Vista), aktueller Antiviren-Software, Firewall und passwortgeschütztem Account sein, dessen Zugangsdaten nur berechtigten Personen bekannt ist und auf dem regelmäßige Datensicherungen vorgenommen werden. Ergänzende Hinweise zur Datensicherheit finden Sie hier.

Die Weitergabe von Dateien sollte ausschließlich verschlüsselt erfolgen.

6. Weitergabe an Externe?

Wenn Sie die Transkription oder Verarbeitung (z.B. Codierung) extern vergeben, so müssen Sie i.d.R. zwingend eine "Vereinbarung zur Auftragsverarbeitung" abschließen. Das gilt auch für externe Hoster oder Dienstleister z.B. bei Online-Befragungen. Insbesondere ist sicherzustellen, dass etwaige Unterbeauftragte ebenfalls die datenschutzrechtlichen Standards einhalten. Allgemeine Hinweise der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Auftragsverarbeitung finden Sie hier.

7. Sicheres Löschen

Achten Sie nach Projektende bzw. der vereinbarten Aufbewahrungsfrist darauf die Daten sicher zu löschen. Das Verschieben in den Papierkorb oder der Löschen-Knopf alleine reichen nicht aus, da die Daten bei „normalem“ Löschen meist ohne großen Aufwand wiederhergestellt werden könnten. Das Bundesamt für Sicherheit und Informationstechnik empfiehlt auf folgender Webseite spezifische und kostenfreie Software zum sicheren Löschen von Daten https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html.

Das gilt auch und insbesondere für die Speicher von Aufnahmegeräten! Besonders, wenn die Geräte ausgeliehen sind (bspw. über die Medienstelle einer Hochschule) müssen die Aufnahmen auch von dort sicher gelöscht werden.

8. Dokumentation

Alle Schritte, inklusive der Löschung etc. sind zu dokumentieren. Wie so eine Dokumentation konkret aussehen muss ist hierbei nicht genauer geregelt. Das kann also eine knappe Excel-Liste oder eine Textdatei sein. Wichtig ist hier, dass Sie bei einer eventuellen Prüfung nachweisen können, dass alle o.g. Punkte bedacht und berücksichtigt wurden.

9. Falls etwas schief geht: Informationspflichten

Sollte ein begründeter Verdacht bestehen, dass Daten verloren wurden oder in die Hände Unbefugter gelangt sind, besteht ggf. die gesetzliche Pflicht, unverzüglich die Aufsichtsbehörde (meist Datenschutzbeauftragte des Landes) und die Personen, deren Daten betroffen sind, zu informieren (ergänzende Informationen stellt das Bayerische Landesamt für Datenschutzaufsicht hier bereit).

Quelle: Thorsten Pehl, Thorsten Dresing: Checkliste Datenschutz 2018, https://www.audiotranskription.de/qualitative-Interviews-DSGVO-konform-aufnehmen-und-verarbeiten