Senatsverwaltung für Bildung,
Jugend und Familie

BERLIN

Anlage 2

Merkblatt zu technisch-organisatorischen Maßnahmen zum Schutz von personenbezogenen bzw. personenbeziehbaren Daten bei an Schulen durchzuführenden Übungen im Forschen nach § 65 Schulgesetz durch Lehramtsstudierende

Auch wenn eine Einwilligung zur Studie und zur Verarbeitung personenbezogener bzw. personenbeziehbarer Daten vorliegt, müssen weitere Maßnahmen zum Schutz getroffen werden. Das sind sogenannte technische und organisatorische Maßnahmen (vgl. Art. 32 der Datenschutz-Grundverordnung). Folgende Punkte müssen bei der Verarbeitung und Nutzung von personenbezogenen bzw. personenbeziehbaren Daten eingehalten werden:

Datenerhebung und -aufbereitung (Anonymisierung und Pseudonymisierung):

- Bild- und Tonaufzeichnungen mit privaten Handys sind nicht erlaubt.
- Personenbezogene Daten sollten so schnell und umfassend wie möglich anonymisiert werden. Wenn Sie bestimmte Inhalte durch Pseudonyme ersetzen, dann wird üblicherweise eine Pseudonymisierungsliste/Schlüsselliste angelegt, die besonders geschützt werden muss.
- Achten Sie bei der Aufbereitung der Daten, dass alle personenbezogenen Daten, aber auch der Schulname oder andere personenbeziehbare Daten anonymisiert oder durch ein Pseudonym ersetzt werden. Nutzen Sie hierfür die von der Universität zur Verfügung gestellte Software.

Datenhaltung und Datensicherheit

- Alle Daten müssen auf der IT-Infrastruktur der Universität abgespeichert werden, das ist meistens eine Cloud. Diese Cloud ist ausreichend geschützt. Das Speichern auf privaten Geräten ist nicht erlaubt. Arbeiten Sie bei der Auswertung auch innerhalb der Cloud.
- Schützen Sie die Dateien vor unberechtigten Zugriffen, in dem Sie sichere Passwörter für Computer- und Speichersysteme verwenden. Nutzen Sie für Ihren Rechner eine Virussoftware und aktivieren Sie eine Firewall.
- Personenbezogene Daten sollten so schnell und umfassend wie möglich anonymisiert oder falls nötig getrennt von den Forschungsdaten aufbewahrt werden. Getrennte Aufbewahrung bedeutet in Ihrem Fall die Speicherung in verschiedenen Ordnern mit unterschiedlichen Zugriffsrechten. Beispielsweise müssen Audioaufnahmen getrennt von den Transkripten und getrennt von den Pseudonymisierungslisten/Schlüssellisten abgespeichert werden.
- Die Einwilligungserklärungen der teilnehmenden Personenkreise verbleiben in der Schule und werden dort in einem verschließbaren Schrank gelagert, bis der Zweck der Studie erfüllt ist. Geben Sie den Schulen unbedingt Bescheid, wenn die Einwilligungserklärungen datenschutzkonform vernichtet/geschreddert werden können.

Datenlöschung und Datennachnutzung

- Wenn die Daten nicht mehr benötigt werden, z. B. weil Sie Ihre Arbeit abgegeben haben, dann löschen Sie die Daten bitte. Sicheres Löschen und Vernichten erfordert, dass die Dateien überschrieben werden. Einfaches Löschen oder Verschieben in den Papierkorb reicht nicht aus, um Daten zu vernichten, wie es etwa für sensible Daten erforderlich sein kann.

- Informieren Sie die Schulen, wenn die Einwilligungserklärungen in den Schulen vernichtet werden können.
- Wenn die Daten von Ihren Dozierenden weitergenutzt werden sollen, dann muss die Weitergabe ausreichend sicher erfolgen, z.B. über das Anlegen eines sicheren, zugriffgeschützten Ordners in der Cloud Ihrer Universität. Kein Verschicken per Mail!
- Sie sind während der Arbeit zuständig für die sichere Speicherung und Verarbeitung der Daten. Sensibilisieren Sie sich und Ihr Verhalten für den sicheren Umgang mit personenbezogenen bzw. personenbeziehbaren Daten.