TOM

Schutzziele der Informationssicherheit:

1. Datenminimierung (Erforderlichkeit für Zweck)
2. Transparenz (Information gem. Art. 13 DSGVO)
3. Nichtverkettung (u.a. Pseudonymisierung, Anonymisierung)

TOM im engeren Sinne:

1. Verfügbarkeit
2. Integrität
3. Vertraulichkeit

Zu 4. Verfügbarkeit (Schutz vor Zerstörung und Verlust, Wiederherstellbarkeit)

* Papier oder/und IT?
  + Papier wo aufbewahrt? (verschlossene Schränke)
  + IT:

- Name IT-Admin

- RRZE-Infrastruktur (bei IT über RRZE Serverpfad, Verweis auf RRZE-TOM) oder

- lokal an der Einrichtung (Servername, externe Festplatten?) oder

- über Drittanbieter? -> AVV (bei größeren Projekten über Referat H3)

- Backup?

- RRZE -> Verweis auf RRZE

- falls lokal; wie, wie oft, wo?

* Ggf.: Ist verwendete Software für
  + Umfrage
  + Audio-/Videoaufnahme
  + Transkription
  + Auswertung
  + etc.

DSGVO-konform? (aus EU, aus Staaten mit Angemessenheitsbeschluss (u.a. Norwegen Schweiz, Kanada), sonst z.B. Standardvertragsklauseln (=SCC) erforderlich, Problemfall USA)

Zu 5. Integrität (Schutz vor Verfälschung der Daten)

Verschlüsselung, Firewall? Zugriff durch Unberechtigte, Putzkräfte, Besucher… verhindert?

Zu 6. Vertraulichkeit (Zugangskontrolle: wer hat Zugang zu welchen Daten?)

* + Welche Rechte des IT-Admin und warum?
  + Rechte und Rollen der Mitarbeiter (z.B. nicht ganzer Lehrstuhl, sondern nur Projektbeteiligte haben Zugriff)
  + Übermittlungsweg an Dritte, falls vorgesehen? (keine Dropbox etc., NUR FAUbox, Verschlüsselung bei Mailübermittlung)

Verarbeitung in FAU-Räumen/Homeoffice?

Nur Dienstgeräte, keine privaten Geräte (siehe IT-Richtlinie)

Schulung des Personals