
DIE REKTORINStabsstelle 7
Datenschutz und IT-Sicherheit

Ihr Zeichen:

Mein Zeichen:

Der Datenschutzbeauftragte
Universitätsstraße 47, Gebäude 9
58097 Hagen
Fon: +49 2331 987-2511
Datenschutzbeauftragter@
fernuni-hagen.de

Datum 05.06.2019

C H E C K L I S T E

Datenschutzprüfung – notwendige Unterlagen

Unterlagen, die dem Datenschutzbeauftragten zur datenschutzrechtlichen Prüfung möglichst **vor Beginn** einer Maßnahme vorgelegt werden sollten:

- I. **(Forschungs-)Konzept** für die Datenverarbeitung (DV) mit folgenden Inhalt:
 1. Wer (Verantwortung, operative Durchführung)?,
 2. Was (welche personenbezogenen Daten, weiteres Material)?,
 3. Wozu (Zweck, Aufgabe)?,
 4. Womit (Art der Verarbeitung, Einsatz von IT-Systemen)?,
 5. Wie (Prozessbeschreibungen)?,
 6. Wie lange (Dauer der Verarbeitung)?
- II. **Verzeichnis der Verarbeitungstätigkeiten (VVT);**
- III. gegebenenfalls Unterlagen zur **Auftragsverarbeitung (AV);**
- IV. **Datenschutzkonzept**, das u. a. eine Dokumentation der Überlegungen enthält, die zur Auswahl der Maßnahmen für Privacy by Design und by Default und zur Datensicherheit geführt haben; darüber hinaus sollte beschrieben werden, wer wann auf welche Daten Zugriff erhält.
- V. **Beschreibung der technischen und organisatorischen Maßnahmen (TOM)** die gewährleisten, dass ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau erreicht wird. Dazu können, abhängig von der geplanten DV, gehören:
 1. **Beschreibung der Verarbeitungsschritte**, die ermöglicht, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
 2. **Maßnahmen zur Sensibilisierung** der an Verarbeitungsvorgängen Beteiligten,
 3. **Beschränkung des Zugangs** zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
 4. **Konzept zur Anonymisierung** (und wenn sie nicht möglich ist) bzw. zur **Pseudonymisierung** personenbezogener Daten,
 5. Maßnahmen zur **Verschlüsselung** personenbezogener Daten,
 6. Beschreibung und Sicherstellung der **Belastbarkeit der Systeme** (inkl. der Vertraulichkeit, Integrität und Verfügbarkeit), die im Zusammenhang mit der Verarbeitung personenbezogener Daten eingesetzt werden,
 7. Beschreibung der Maßnahmen, die die Verfügbarkeit und den Zugang bis zur **Wiederherstellung der Daten** bei einem physischen oder technischen Zwischenfall sicherstellen,
 8. die Einrichtung eines **Verfahrens zur regelmäßigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung,
 9. **spezifische Verfahrensregelungen**, die im Falle einer **Übermittlung** oder **Verarbeitung für andere Zwecke** die Einhaltung der Vorgaben der DSGVO sicherstellen.