**Fragebogen zur Ersterfassung von Verarbeitungen**

**Wichtiger Hinweis:** Es müssen nicht alle Fragen beantwortet werden. Bitte geben Sie den Fragebogen auch dann ab, wenn Sie nur einen Teil der Fragen beantworten können.

**Erster Abschnitt: Fragen zur Beschreibung der Verarbeitung:**

1. **Kurzbeschreibung der Verarbeitung:** (z.B. Ehemaligenverwaltung, Bewerberverwaltung, Befragung zur Nutzung von Social Media, etc.)
2. **Welche Zwecke verfolgt die Verarbeitung? Bitte beschreiben Sie diese möglichst genau mit eigenen Worten.**
3. **Welche Stelle oder welche Person entscheidet auf operativer Ebene innerhalb der Hochschule über das Ob und den Umfang der Verarbeitung und wer hat welchen Zugriff?**
4. **Wessen Daten werden verarbeitet? Hierbei reicht die Angabe von Personengruppen.**

*Beispiele: Studierende, Studierende des Fachbereichs Sozialwissenschaften, Studienbewerber, Umfrageteilnehmer, Ehemalige Studierende, Ehemalige Mitarbeiter, etc.*

1. **Welche Informationen werden von den in 4. genannten Personen verarbeitet? Bitte geben sie die Informationen je Personengruppe an. Werden von mehreren Personengruppen identische Informationen verarbeitet, können die Angaben einfach zusammengefasst werden.**

*Beispiele:*

*Studienbewerber: Name, Anschrift, Private E-Mail, Telefon, Note Allgemeine Hochschulreife*

*Studierende, Ehemalige Studierende: Name, Anschrift, Matrikelnummer*

**Hinweis: Hier muss geprüft werden, ob zu den oben genannten Zwecken gegebenenfalls auch pseudonymisierte Daten ausreichen.**

**Hinweis: Anhand der angegebenen Daten muss geprüft werden, ob besondere Kategorien von personenbezogenen Daten verarbeitet werden.**

1. **Werden die Informationen für ein Scoring, für automatisierte Entscheidungen verwendet? Werden die Informationen über eine Videoüberwachung gewonnen?**
2. **Ist die Rechtsgrundlage der Datenverarbeitung bekannt? Diese kann sich z.B. aus einer informierten Einwilligung oder einem Gesetz ergeben, das die Verarbeitung erlaubt oder gar zu der Verarbeitung verpflichtet.**
3. **Haben Stellen oder Partner außerhalb der Hochschule Zugriff auf oder Einsicht in die Daten**

**Wenn nein: Weiter mit 9., ansonsten:**

**8.1 Bestehen vertragliche Vereinbarungen mit den Stellen/Partnern?**

**Hinweis: Wenn ja muss geprüft werden, ob die geprüfte Vorlage verwendet wurde. Im Zweifel muss eine Prüfung durch die Rechtsabteilung oder den bDSB erfolgen.**

 **Wenn nein: Erfolgt der Zugriff oder die Einsichtnahme aufgrund eines Gesetzes?**

 **8.2 Sitzt eine der Stellen oder ein Partner außerhalb der EU?**

 **Wenn ja: In welchem Land?**

**Hinweis: Besteht für dieses Land kein Angemessenheitsbeschluss muss hier eine erweiterte Prüfung durch den bDSB oder die Rechtsabteilung erfolgen**

1. **Werden die Daten an andere interne Stellen weitergegeben?**

**Wenn ja: erfolgt dies für die oben genannten Zwecke oder erfolgt dies für andere Zwecke? Hinweis: Wenn ein anderer Zweck verfolgt wird, muss geprüft werden, ob die damit verbundene Zweckänderung mit dem Ursprungszweck vereinbar ist. Zudem muss die andere interne Stelle diese Verarbeitung beschreiben.**

1. **Erhalten Sie die Daten direkt von den betroffenen Personen oder erhalten Sie diese von einer internen oder externen Stelle?**

**Hinweis: Bei einer internen Stelle muss geprüft werden, ob der gleiche Zweck verfolgt wird. Wird der gleiche Zweck verfolgt wurde die Verarbeitung gegebenenfalls schon durch die andere Stelle dokumentiert. Wenn nein, muss dies von der intern für die Verarbeitung verantwortlichen Stelle nachgeholt werden**

**Hinweis: Bei einer externen Stelle muss der Betroffene im Rahmen der Informationspflichten spätestens nach einem Monat darauf hingewiesen werden, woher seine Daten stammen. Ansonsten ist ihm dies schon früher mit der ersten Ansprache oder bei einer beabsichtigten Weiterübermittlung an Externe mitzuteilen.**

1. **Gibt es feste Fristen zur Löschung von personenbezogenen Daten oder zu deren Anonymisierung?**

**Wenn nein: Unter welchen Umständen ist die Löschung/Anonymisierung vorgesehen.**

1. **Gibt es bereits einen Plan für den Fall, dass die Verarbeitung ganz eingestellt wird? Werden Daten noch für eine gewisse Zeit aufbewahrt? Erfolgt eine Bereinigung der zur Verarbeitung genutzten Systeme?**

**Zweiter Abschnitt: Fragen zur Umsetzung der Betroffenenrechte**

1. **Wie werden die Betroffenen an einer geeigneten Stelle über Zweck, Rechtsgrundlage, Umfang und Dauer der Verarbeitung ihrer Daten informiert?**
2. **Kann technisch oder manuell eine Kopie sämtlicher zu einer Person gespeicherter Daten erzeugt werden? In welchen Formaten ist dies möglich und wer von den Zugriffsberechtigten kann dies realisieren?**

**Hinweis: Dies dient der Prüfung, ob das Betroffenenrecht auf Auskunft realisierbar ist.**

1. **Können im Bedarfsfall Daten zu einer Person korrigiert werden? Wenn ja: Wer hat die Berechtigung zu Korrekturen?**

**Dritter Abschnitt: Fragen zu technischen und organisatorischen Sicherheitsmaßnahmen**

1. **Auf welchen Systemen und unter Verwendung welcher Programme werden die Daten gespeichert und zu den oben genannten Zwecken verarbeitet? Bitte beschreiben Sie dies mit eigenen Worten möglichst genau.**
2. **Werden Backups/Sicherungen erstellt?**

 **Wenn ja: Wie lange werden diese aufbewahrt?**

1. **Wurden besondere Maßnahmen zur Sicherheit ergriffen? Bitte beschreiben Sie diese mit eigenen Worten. Sie können sich hierbei an den Beispielen in Anlage 1 orientieren.**
2. **Welche Vorgänge werden automatisch oder manuell protokolliert und wie lange werden die Protokolle aufbewahrt?**

*Beispiel: lesende, schreibende, ändernde Zugriffe werden für x Monate gespeichert, wobei die jeweils ältesten Protokolle überschrieben werden.*

## Anlage 1: Beispielhafte Nennung von Maßnahmen für die Sicherheit zur Beantwortung von Frage 18

## Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

* Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
* Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
* Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
* Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit
* Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

## Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

* Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
* Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

## Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

* Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
* Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);