** **

**  **

Fragebogen zur Ersterfassung von Verarbeitungen

Erweiterte Fassung, Version 2.0, 21.02.2019

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0

<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>

Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO) −
Datenschutzmanagementsysteme“ 2018

gefördert vom 

Fragebogen zur Ersterfassung von Verarbeitungen

Bitte beantworten Sie so viel Fragen wie möglich und geben Sie den Fragebogen auch dann ab, wenn Sie nur einen Teil der Fragen beantworten können.

1. Abschnitt: Fragen zur Organisationseinheit

1. Was ist die Kerntätigkeit der Organisationseinheit? Bitte beschreiben sie diese kurz in eigenen Worten:

Bei Forschungsvorhaben bitte die Fakultät/Wissenschaftliche Einrichtung angeben

|  |
| --- |
|  |

1. Sind in nächster Zukunft Umstrukturierungen in der Organisationseinheit zu erwarten?

|  |
| --- |
|  |

2. Abschnitt: Fragen zur Beschreibung der Verarbeitung:

1. Kurzbeschreibung der Verarbeitung:

Beispiele: Ehemaligenverwaltung, Bewerberverwaltung, Befragung zur Nutzung von Social Media, etc.

|  |
| --- |
|  |

1. Welche Zwecke verfolgt die Verarbeitung? Bitte beschreiben Sie diese möglichst genau mit eigenen Worten.

Beispiel: Das Serviceverfahren ist ein System zur Koordinierung...

|  |
| --- |
|  |

1. Welche Stelle oder welche Person innerhalb der Universität entscheidet auf operativer Ebene über das Ob und den Umfang der Verarbeitung? Bitte benennen Sie einen Verfahrensverantwortlichen.

|  |
| --- |
|  |

1. Gibt es eine/n Datenschutz und Informationssicherheitskoordinator\*in (DISK) in Ihrer Organisationseinheit? Wenn ja, bitte geben Sie Namen und Kontaktdaten an.

|  |
| --- |
|  |

1. Bitte nennen Sie Name und Kontaktdaten des inhaltlichen Ansprechpartners der Organisationseinheit. Falls es diesen noch nicht gibt, muss dieser zeitnah benannt werden.

|  |
| --- |
|  |

1. Wessen Daten werden verarbeitet? Hierbei reicht die Angabe von Personengruppen.

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

|  |
| --- |
|  |

1. Welche personenbezogenen Daten werden von den in 6. genannten Personen verarbeitet? Bitte geben sie die Daten 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

Ehemalige Studierende: Name, Anschrift, Datum des Studienabschlusses

|  |
| --- |
|  |

1. Führen Sie Scoring, automatisierte Entscheidungen oder Videoüberwachung durch? Wenn ja, für welchen Zweck und welche Daten/Datenkategorien sind davon betroffen?

|  |
| --- |
|  |

1. Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Bitte benennen Sie diese jeweils für jede Verarbeitung personenbezogener Daten.

Beispiel gesetzliche Grundlagen (DSGVO, DSG NRW; HG NRW; HGB etc.), Einwilligungen usw.

|  |
| --- |
|  |

1. Werden personenbezogene Daten an andere interne Stellen weitergegeben?

**Wenn ja**, **an welche interne Stelle/n? Wenn ja, erfolgt dies für die oben genannten Zwecke oder erfolgt dies für andere Zwecke?**

|  |
| --- |
|  |

1. Werden personenbezogene Daten an externe Stellen oder Partner außerhalb der Universität weitergegeben? Wenn ja, auf welcher Grundlage?
	1. Bestehen vertragliche Vereinbarungen mit den Stellen/Partnern? Wenn ja, um welche Verträge handelt es sich (Dienstvertrag, AV-Vertrag nach Art. 28 DS-GVO, gemeinsame Verantwortlichkeit nach Art. 26 usw.)?

|  |
| --- |
|  |

* + - Wenn es sich um einen AV-Vertrag nach Art. 28 DS-GVO handelt: sind Sie Auftraggeber oder Auftragnehmer?

|  |
| --- |
|  |

* + - Wenn es sich um eine gemeinsame Verantwortlichkeit handelt: Name und Kontaktdaten des weiteren Verantwortlichen

|  |
| --- |
|  |

* + - **Wenn es sich nicht um eine vertragliche Grundlage handelt: Erfolgt die Weitergabe aufgrund eines Gesetzes?**

|  |
| --- |
|  |

* 1. Sitzt eine der Stellen oder ein Partner ausschließlich außerhalb der EU? Wenn ja: In welchem Staat?

|  |
| --- |
|  |

1. Haben interne Stellen (universitätsintern) oder externe Stellen – unabhängig von einer Weitergabe nach Ziff. 10 und 11 – Zugriffsberechtigungen auf die personenbezogenen Daten? Wenn ja, welche Personen/Stellen?

|  |
| --- |
|  |

1. Woher stammen die von Ihnen verarbeiteten personenbezogenen Daten: werden diese unmittelbar beim Betroffenen (d.h. in der Regel direkt beim Studierenden oder Beschäftigten) oder erhalten Sie die Daten von anderen internen oder externen Stellen? Bitte nennen Sie Ihre (jeweiligen) Datenquellen?

|  |
| --- |
|  |

1. Gibt es definierte Fristen zur Löschung von personenbezogenen Daten oder zu deren Anonymisierung? Bitte um Angabe der Zeitdauer (in Tagen, Monaten oder Jahren). Wenn nein: Unter welchen Umständen ist die Löschung/Anonymisierung vorgesehen?

|  |
| --- |
|  |

1. Ist eine Datenschutzfolgenabschätzung (DSFA) geplant?

|  |
| --- |
|  |

1. Gibt es Absichten, dass die Verarbeitungstätigkeit komplett eingestellt wird?

Beispiele: Forschungsvorhaben läuft aus; Organisationseinheit wird umstrukturiert oder fusioniert mit anderer Einheit etc.

|  |
| --- |
|  |

3. Abschnitt: Fragen zur Umsetzung der Betroffenenrechte

1. Wie werden die Betroffenen gemäß Art. 13 + 14 DS-GVO (über Zweck, Rechtsgrundlage, Umfang, Dauer usw. der Verarbeitung ihrer Daten) informiert?

|  |
| --- |
|  |

1. 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 jederzeit Daten zu einer Person korrigiert werden? Wenn ja: Wer hat die Berechtigung zu Korrekturen?

|  |
| --- |
|  |

4. 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.

|  |
| --- |
|  |

1. 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.

|  |
| --- |
|  |

1. 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.

|  |
| --- |
|  |

5. Abschnitt: Schutzbedarffeststellung

Eine Schutzbedarffeststellung dient dazu in einem ersten Schritt festzustellen, wie hoch der Schutzbedarf bestimmter Daten ist, ausgehend vom potenziellen Schaden, der beim missbräuchlichen Umgang mit diesen Daten entstehen kann.

Bitte überlegen Sie sich, wie hoch der zu erwartende Schaden beim missbräuchlichen Umgang mit den im Verfahren verarbeiteten Daten (je nach Kategorie und Bedrohungzenario) wäre (Tabelle 1). Tragen Sie die Ergebnisse Ihrer Einschätzung in die Tabelle 2.

# Bewertungsmatrix für den Schutzbedarf (Tabelle 1)

|  |  |  |
| --- | --- | --- |
| **Beeinträchtigung Kategorie** | **Bedrohung** | **Folgen des Schadens** |
| 1. Beeinträchtigung der Aufgabenerfüllung | Missbrauch der Daten  | Für alle Benutzer des Systems tolerierbar…führt maximal zum Ausfall einzelner Arbeitsabläufe (tolerierbare Ausfallzeit mehr als einen Arbeitstag). | Für einzelne Benutzer des Systems nicht tolerierbar…schränkt die Aufgabenerfüllung in einem Teilbereich ein (tolerierbare Ausfallzeit zwischen einer und 24 Stunden). | Für alle Benutzer des Systems nicht tolerierbar…gefährdet den Gesamtauftrag der Universität (tolerierbare Ausfallzeit weniger als eine Stunde). |
| Manipulation der Daten |
| Verlust der Daten  |
| 2. Negative Innen- und/oder Außenwirkung | Missbrauch der Daten | **Geringer** Ansehens- und Vertrauensverlust eines Teilbereichs der Universität | Ansehens- und Vertrauensverlust der Universität bei einer **eingeschränkten** ÖffentlichkeitoderHoher Ansehensverlust eines Teilbereichs der Universität | **Landesweiter** Ansehens und Vertrauensverlust der Universität in der **breiten** Öffentlichkeit |
| Manipulation der Daten |
| Verlust der Daten |
| 3. Finanzielle Auswirkungen | Missbrauch der Daten | Finanz. Schaden weniger als ca. 150.000€  | Finanz. Schaden weniger als ca. 3 Millionen € | Finanz. Schaden mehr als ca. 3 Millionen €  |
| Manipulation der Daten |
| Verlust der Daten |
| 4. Beeinträchtigung der persönlichen Unversehrtheit | Missbrauch der Daten | ...erscheint nicht möglich | ...kann nicht absolut ausgeschlossen werden | Gravierende Auswirkungen sind möglich (Gefahr für Leib und Leben). |
| Manipulation der Daten |
| Verlust der Daten |
| 5. Verstoß gegen Gesetze, Vorschriften und/oder Verträge | Missbrauch der Daten | ...verstößt gegen Gesetze oder Vorschriften mit **geringen** Konsequenzen...hat geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge. | ...verstößt gegen Gesetze oder Vorschriften mit **erheblichen** Konsequenzen....hat Vertragsverletzungen mit hohen Konventionalstrafen und/oder erheblichen Haftungsschäden zur Folge. | ...verstößt **fundamental** gegen Gesetze oder Vorschriften...hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die Uni ruinös sind. |
| Manipulation der Daten |
| Verlust der Daten |
| **Notwendiger Schutzbedarf:** | **normal** | **hoch** | **sehr hoch** |

# Ergebnisse der Bewertungsmatrix (Tabelle 2)

|  |  |  |
| --- | --- | --- |
| **Beeinträchtigungen (Kategorien)** | **Bedrohung** | **Abschätzung des Schadens** |
| 1. Beeinträchtigung der Aufgabenerfüllung | Missbrauch der Daten |  |  |  |
| Manipulation der Daten |  |  |  |
| Verlust der Daten |  |  |  |
| 2. Negative Innen- und/oder Außenwirkung | Missbrauch der Daten |  |  |  |
| Manipulation der Daten |  |  |  |
| Verlust der Daten |  |  |  |
| 3. Finanzielle Auswirkungen | Missbrauch der Daten |  |  |  |
| Manipulation der Daten |  |  |  |
| Verlust der Daten |  |  |  |
| 4. Beeinträchtigung der persönlichen Unversehrtheit | Missbrauch der Daten |  |  |  |
| Manipulation der Daten |  |  |  |
| Verlust der Daten |  |  |  |
| 5. Verstoß gegen Gesetze, Vorschriften oder Verträge | Missbrauch der Daten |  |  |  |
| Manipulation der Daten |  |  |  |
| Verlust der Daten |  |  |  |
| **Notwendiger Schutzbedarf:** | **normal** | **hoch** | **sehr hoch** |

# 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);