Sachbericht:
Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO):
Datenschutzmanagementsysteme Phase II –
Handreichungen und praktische Umsetzung

|  |  |
| --- | --- |
| **Zuwendungsempfängerin:** | Universität Paderborn, Warburger Str. 100, 33098 Paderborn |
| **Beteiligte Hochschulen:** | Universität Bielefeld, Fachhochschule Bielefeld, Universität Paderborn, Universität Siegen |
| **Berichtszeitraum:** | 13.06.2018 bis 31.12.2018 |
| **Aktenzeichen:** | 214 – 5.01.06.01.03 - 137349 |

Seit dem 25. Mai 2018 gelten die EU-Datenschutz-Grundverordnung (DSGVO)[[1]](#footnote-1) und das novellierte Landesdatenschutzgesetz Nordrhein-Westfalen (DSG NRW)[[2]](#footnote-2). Vor dem Hintergrund der neuen Gesetzgebung − insbesondere der in der DSGVO geforderten „Rechenschafts- und Nachweispflichten“ − wurde in einer ersten Projektphase 2017 mit der Konzeption eines Datenschutzmanagementsystems (DSMS) begonnen.

Ausgehend von der in Phase I entworfenen Datenschutzleitlinie und des Datenschutzkonzepts wurden in Phase II 2018 im Schwerpunkt Musterprozesse entwickelt und Handreichungen erarbeitet, um die Hochschulen bei der Umsetzung der DSGVO zu unterstützen. Dabei wurde von den folgenden Handlungsfeldern ausgegangen.



3

9

6

2

1

8

7

5

4

Handlungsfelder, um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sicherzustellen

# Ergebnisse des Projekts (Handreichungen, Dokumente)

## Verfahrensdokumentation / Verzeichnis von Verarbeitungstätigkeiten (VVT)

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO bildet die Basis eines Datenschutzmanagementsystems. Das VVT muss vom Verantwortlichen (ebenso vom Auftragsverarbeiter) für jede in seinem Verantwortungsbereich stattfindende Verarbeitung personenbezogener Daten erstellt werden. Es ist die Grundlage für die verfahrensspezifische Rechenschaftspflicht. Dazu bietet es sich an Informationen in das VVT aufzunehmen, die über die Anforderungen des Art. 30 hinausgehen.

* Grundlagen für die Erstellung von Verzeichnissen der Verarbeitungstätigkeiten
(Grundlagen\_VVT\_Projekt-DSMS\_v1.0)
* Fragebogen zur Ersterfassung von Verarbeitungstätigkeiten
(Fragebogen\_Ersterfassung\_Verarbeitungstaetigkeiten\_Projekt-DSMS\_v1.0)
* Erweiterter Fragebogen zur Ersterfassung von Verarbeitungstätigkeiten
(Erweiterter\_Fragebogen\_Ersterfassung\_Verarbeitungstaetigkeiten\_Projekt-DSMS\_v2.0)
* Musterformular VVT für die Hochschule als Verantwortlicher
(Muster\_VVT\_Verantwortlicher\_Projekt-DSMS\_v1.0)
* Musterformular VVT für die Hochschule als Auftragsverarbeiter
(Muster\_VVT\_Auftragsverarbeiter\_Projekt-DSMS\_v1.0)
* Ausfüllhilfe für das VVT für die Hochschule als Verantwortlicher
(Ausfuellhinweise\_VVT\_Verantwortlicher\_\_Projekt-DSMS\_v1.0)
* Übersicht über Verarbeitungen mit personenbezogenen Daten sowie AV-Verträge
(Uebersichtsliste\_Verarbeitungen\_sowie\_AV-Vertraege)

## proaktive Informationspflichten

Betroffene Personen müssen gemäß Art. 12ff DSGVO über jede Verarbeitung ihrer personenbezogenen Daten transparent sowie in einer verständlichen und leicht zugänglichen Form informiert werden. Dies kann über klassische papierbasierte Informationsblätter erfolgen, aber auch elektronisch bspw. über webbasierte Datenschutzerklärungen.

* Muster Datenschutzhinweise
(Muster\_Datenschutzhinweise\_\_Projekt-DSMS\_v1.0,
Muster\_Entwurf\_Datenschutzhinweise\_einfache\_Sprache\_\_Projekt-DSMS\_v1.0)
* Beispiele/Muster: Datenschutzhinweise / Datenschutzerklärungen / Informationsblätter

## Betroffenenrechte (Auskunft)

Über die Informationspflichten hinaus müssen vom Verantwortlichen die weiteren Betroffenenrechte gewahrt und bei Anfragen innerhalb einer Frist von einem Monat umgesetzt werden. Das betrifft neben Löschung, Berichtigung und Einschränkung der Verarbeitung insbesondere auch das Auskunftsrecht der betroffenen Person gemäß Art. 15 DSGVO.

* Musterprozess und Hinweise zur Erteilung von Auskunft an betroffene Personen
(Musterprozess\_und\_Hinweise\_\_Auskunft\_an\_Betroffene\_\_Projekt-DSMS\_v2.0)

## Schwellwertanalyse und Datenschutz-Folgenabschätzung

Besteht für eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, so muss der Verantwortliche gemäß Art. 35 DSGVO die Risiken im Rahmen einer Datenschutz-Folgen­ab­schätzung bewerten und basierend auf den Ergebnissen geeignete Maßnahmen zur Bewältigung der Risiken ergreifen. Das voraussichtliche Bestehen von Risiken lässt sich im Rahmen einer datenschutzrechtlichen Schwellwertanalyse sowie der informationssicherheitstechnischen Schutzbedarfsfeststellung abschätzen.

* DSFA: Datenschutz-Folgeabschätzung − Grundlagen, Methodik
(DSFA\_Grundlagen\_Methodik\_\_Projekt-DSMS\_v1.0)

## Technische und organisatorische Maßnahmen (TOM)

Der Sicherheit der Verarbeitung wird in der DSGVO einen besonderer Stellenwert eingeräumt. Neu sind dabei die Grundsätze Technikgestaltung (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default) gemäß Art. 25 DSGVO. Die Sicherheit der Verarbeitung muss durch geeignete technische und organisatorische Maßnahmen gewährleistet werden, die über die klassischen informationssicherheitstechnischen Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität hinausgehen (Art. 32 DSGVO). Weiter sind Verfahren für die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zu etablieren (Art. 24 DSGVO).

* Technische und organisatorische Maßnahmen entsprechend der Vorgaben der EU-DSGVO und dem DSG NRW n. F. − Handreichung zu TOMs in Anlehnung an den BSI-Grundschutz
(Handreichung\_TOMs\_Projekte\_DSMS\_und\_Sensibilisierung\_v1.0)
* TOM-Muster für verschiedene Anwendungsfälle
(Muster\_TOMs\_in\_Anlehnung\_an\_LDI\_\_Projekt-DSMS\_v1.0,
Muster\_TOMs\_fuer\_kleines\_Forschungsprojekt\_Projekt-DSMS\_v1.0,
Muster\_TOMs\_in\_Anlehnung\_an\_ZENDAS\_\_Projekt-DSMS\_v1.0)

## Meldung von Datenschutzverletzungen

Wird die Sicherheit eines Systems / einer Verarbeitung kompromittiert und kommt es dadurch zu einer Verletzungen des Schutzes personenbezogener Daten, so muss diese vom Verantwortlichen (unverzüglich und möglichst binnen 72 Stunden) an die Aufsichtsbehörden gemeldet werden (Art. 33 DSGVO).

* Muster eines Rundschreibens an alle Beschäftigten zur Meldung von Datenschutzverletzungen
(Muster\_Rundschreiben\_an\_Beschaeftigte\_zu\_Datenschutzverletzungen\_\_Projekt-DSMS)
* Musterformular zur hochschulinternen Meldung möglicher Datenschutzverletzungen
(Musterformular\_Interne\_Meldung\_Datenschutzverletzung\_\_Projekt-DSMS\_v1.0)
* Musterformular zur Dokumentation gemeldeter möglicher Datenschutzverletzungen
(Musterformular\_Dokumentation\_Datenschutzverletzung\_\_Projekt-DSMS\_v1.0)
* Handreichung zur Benachrichtigung Betroffener bei Datenschutzverletzungen gemäß Art. 34:
Checkliste für Verantwortliche zur Formulierung des Informationstextes
(Handreichung\_zur\_Benachrichtigung\_Betroffener\_bei\_Datenschutzverletzungen\_\_Projekt-DSMS\_v2.0)
* Musterprozesse
(Entwurf\_Prozessmodellierung\_Meldepflicht\_Datenschutzverletzung\_Projekt-DSMS,
Muster\_Prozess\_Datenschutzverletzung\_Uebersicht\_\_Projekt-DSMS,
Muster\_Prozess\_Datenschutzverletzung\_Detail\_\_Projekt-DSMS)

## Rechtmäßigkeit

Jede Verarbeitung personenbezogener Daten muss die datenschutzrechtlichen Grundsätze (Art. 5 DSGVO) einhalten und rechtmäßig erfolgen, d. h. es muss eine von sechs vorgegebenen Bedingungen erfüllt sein (Art. 6 DSGVO, Abs. 1):

1. Einwilligung der betroffenen Person in die Verarbeitung
2. Erforderlich zur Erfüllung eines Vertrags mit der betroffenen Person
3. Erfüllung rechtlicher Verpflichtungen
4. Wahrung lebenswichtiger Interessen der betroffenen Person
5. Wahrnehmung einer Aufgabe, die im öffent­lichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
6. Berechtigtes Interesse des Verarbeiters (nicht für Behörden in Erfüllung ihrer Aufgaben)

### Einwilligungserklärungen

Für die Verarbeitung von personenbezogenen Daten muss, sofern keine Rechtsgrundlage gemäß (Art. 6 DSGVO, Abs. 1, lit. b.−f.) vorliegt, im Vorfeld, spätestens aber bei der Datenerhebung, eine Einwilligung der betroffenen Person eingeholt werden (Art. 7 DSGVO). Damit eine Einwilligung rechtskräftig ist, muss sie freiwillig erteilt werden und informiert sowie in Form einer eindeutig bestätigenden Handlung erfolgen.

* Anforderungen an eine informierte Einwilligung (gemäß Art. 7, 8 und 12, 13 DSGVO)
(Anforderungen\_Einwilligung\_\_Projekt-DSMS\_v1.0)
* Einwilligung in die Übermittlung personenbezogener Daten in Drittländer (gemäß Art. 49 DSGVO)
(Einwilligung\_Uebermittlung\_Drittland\_Art\_49\_Projekt-DSMS\_v1.0)
* Muster Einwilligungserklärungen

### Auftragsverarbeitung

Werden Daten durch Dritte im Auftrag eines Verantwortlichen verarbeitet, so ist ein geeigneter Auftragsverarbeiter auszuwählen und es ist eine Vereinbarung zu schließen (Art. 28 DSGVO).

* Checkliste zur Prüfung „externer“ Verträge
(Handreichung\_AV-Vertragspruefung\_\_Projekt-DSMS\_v2.0)
* Muster eines AV-Vertrags
(Mustervertrag\_Auftragsverarbeitung\_\_ZENDAS\_Projekt\_DSMS\_v3.0)
* Auftragsvereinbarung in Ausschreibungsprozessen
(Mustervertrag\_Auftragsvereinbarung\_Ausschreibungsverfahren\_\_Projekt-DSMS\_v1.0,
Begleittext\_Mustervertrag\_Auftragsvereinbarung\_Ausschreibungsverfahren\_\_Projekt-DSMS\_v1.0)

### Gemeinsame Verantwortlichkeit / Joint Controller

Werden die Zwecke und Mittel einer Verarbeitung gemeinsam festgelegt, so besteht eine gemeinsame Verantwortlichkeit und die Partner müssen transparent festlegen, wer welche datenschutzrechtlichen Aufgaben und Pflichten übernimmt (Art. 26 DSGVO).

* Checkliste Gemeinsame Verantwortlichkeit
(Checkliste\_Gemeinsam\_Verantwortliche\_\_Projekt-DSMS\_v1.0)
* Mustervertrag Gemeinsame Verantwortlichkeit
(Mustervertrag\_Gemeinsam\_Verantwortliche\_\_Projekt-DSMS\_v1.0)

## Sensibilisierung und Schulung

Alle Beschäftigten, die mit der Verarbeitung personenbezogener Daten befasst oder daran beteiligt sind, müssen hinsichtlich des Datenschutzes sensibilisiert und geschult werden. Die Umsetzung muss durch den Datenschutzbeauftragten überprüft werden (Art. 39. DSGVO). Hierzu wurden in einem parallelen IuK-Projekt zur „Erstellung eines Sensibilisierungskonzeptes“ personalisierte und zielgruppengerechte Materialien erstellt, u. a. eine E-Learning-Einheit zu Grundlagen des Datenschutzes. Mit dem Sensibilisierungsprojekt fand ein intensiver Austausch statt. Im Projekt Datenschutzmanagementsysteme wurden punktuell Rundschreiben, Folien zur Unterrichtung u. ä. erstellt.

## Rechenschaftspflicht

### Datenschutzleitlinie

In der Datenschutzleitlinie werden die Datenschutzziele in der Hochschule festgelegt, beispielsweise der Aufbau eines Datenschutzmanagementsystems. Sie bildet das Selbstverständnis der Hochschule bezüglich der Umsetzung des Datenschutzes ab und dient als Orientierungshilfe für Entscheidungen. Die Leitlinie muss von der Hochschulleitung als Vertreter des Verantwortlichen verabschiedet und getragen werden.

* Datenschutzleitlinie als Komponente eines Datenschutzmanagementsystems
(Datenschutzleitlinie\_als\_Komponente\_eines\_Datenschutzmanagementsystems\_\_Projekt\_DSMS)
* Muster einer Datenschutzleitlinie
(Muster\_Datenschutzleitlinie\_\_Projekt-DSMS\_v1.0)

### Datenschutzkonzept

Ein Datenschutzkonzept konkretisiert die Vorgaben der Datenschutzleitlinie. Dort werden die Organisationsstruktur und Verantwortlichkeiten sowie die Prozesse zur Umsetzung der datenschutzrechtlichen Vorgaben behandelt.

* Datenschutzkonzept als Komponente eines Datenschutzmanagementsystems
(Datenschutzkonzept\_als\_Komponente\_eines\_Datenschutzmanagementsystems\_\_Projekt\_DSMS)
* Datenschutzkonzept nach den Anforderungen der DSGVO
(Muster\_Datenschutzkonzept\_\_Projekt-DSMS\_v2.0)

### Rollen und Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz obliegt der Hochschulleitung. Die Verantwortung kann zusammen mit den Aufgaben der Datenverarbeitung delegiert werden. Zusätzlich gibt es weitere Rollen, beispielsweise den Informationssicherheitsbeauftragten oder die in Art. 37 DSGVO festgelegte Rolle des Datenschutzbeauftragten.

* Muster-Richtlinie: Rollen und Verantwortlichkeiten für Verarbeitungen nach Art. 5 Art. 2 DSGVO
(Muster\_Richtlinie\_Rollen\_und\_Verantwortlichkeiten\_\_Projekt-DSMS\_v1.0)

## Präsentationen / Folien des Projekts

* Vorträge des Projekts
* Präsentationen in Schulungen
* Folien zu einzelnen Themenbereichen

# Resümee

Abweichend von der Planung wurden noch keine Handreichungen mit allen Details für die Durchführung von Datenschutz-Folgenabschätzungen erstellt. Hier konkurrieren immer noch unterschiedliche Vorgehensweisen (insb. Vorgehen nach Standarddatenschutzmodell (SDM) oder den Vorgaben der französischen Behörde (Commission Nationale de l’Informatique et des Libertés – CNIL) und die Aufsichtsbehörden haben noch keine abschließenden Empfehlungen abgegeben.

Die erstellten Handreichungen, Muster und Vorlagen wurden für die Datenschutzbeauftragten der NRW-Hochschule bereits im Verlauf ihrer Entstehung in Vorversionen auf dem Dokumentenaustauschserver BSCW abgelegt und mit anderen Datenschutzbeauftragten diskutiert.

Das Interesse an den Projektergebnissen ist groß, die Projektmitarbeiter präsentierten das Projekt in verschiedenen Kontexten:

20. November 2018: Eingeladener Vortrag im Rahmen der 7. DFN-Konferenz Datenschutz in Hamburg

25 Februar 2019: Sachstandsbericht zum Projekt im Erfahrungsaustausch der DV-Projektgruppe

7. Mai 2019: Eingeladener Vortrag im Rahmen der 14. Tagung der DFN-Nutzergruppe Hochschulverwaltung − Campus digital? Aber sicher!“ in Ulm

Am 3. und 4. Dezember 2018 fand im Arcadeon in Hagen ein über die HÜF organisierter Abschlussworkshop des Projekts statt, an dem insbesondere die Datenschutzbeauftragten der NRW-Hochschulen teilnahmen. Dort wurden die Projektergebnisse vorgestellt und diskutiert. Am Austausch nahmen auch Vertreter des IuK-Projekts „Erstellung eines Sensibilisierungskonzeptes zur Erfüllung der Anforderungen aus der EU-DSGVO“ teil. Gemeinsam wurden abschließend Ideen für weitere gemeinsame Aktivitäten gesammelt, die vom Sprecherkreis der Datenschutzbeauftragten der Hochschulen in NRW weiter verfolgt werden sollen.

Die Ergebnisse des Projekts und die erstellte Dokumentation werden anderen Hochschulen zur Verfügung gestellt, u. a. über die Angebote der Informations- und Kommunikationstechnik in den Hochschulverwaltungen NRW (IUK-NRW) im Ilias Bildungsforum der Hochschulübergreifenden Fortbildung (HÜF-NRW).

1. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1462345886854&uri=OJ:JOL\_2016\_119\_R\_0001 [↑](#footnote-ref-1)
2. Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) vom 17. Mai 2018, https://recht.nrw.de/lmi/owa/br\_text\_anzeigen?v\_id=3520071121100436275 [↑](#footnote-ref-2)