Anlage 10: Datenschutzfolgenabschätzung DSFA **teilweise separat**

DSFA-Bericht
Bericht der Hochschule Aalen
zur Datenschutz-Folgenabschätzung (DSFA)
für den Verarbeitungsvorgang

DigiExam

Inhalt

1. Information zur DSFA

1.1 Beteiligte Personen und Status

1.1.1 An DSFA beteiligte Person(en) und ihre Rolle(n)	1.1.2 Status der DSFA	1.1.3 Anmerkung zum Status
(Justiziarin und DSB) (Stabsstelle Datenschutz) (Canvas Kernteam) (Canvas Kernteam)	☒ in Bearbeitung ☐ Aktiviert ☐ Deaktiviert	

1.1.4 Kontaktdaten Datenschutzbeauftragte/r

Hochschule Aalen
– Datenschutzbeauftragte –
Beethovenstraße 1
73430 Aalen
datenschutz@hs-aalen.de

1.2 Anlagen bzw. Verweise zum DSFA-Bericht

Nr.	Bezeichnung der Anlage bzw. des Verweises	Quelle und Anmerkung
1	Auftragsverarbeitungsvertrag DigiExam	Anhangsverzeichnis Punkt 2
2	Speicherdauer / Löschfristen DigiExam	DigiExam_05_Löschfristen.xlsx
3	Infoschreiben DigiExam	Anhangsverzeichnis Punkt 7
4	Risikoanalyse Datensicherheitsziele	DSFA-Risikomanagement_DigiExam_v1.0.xlsx
5	Risikoanalyse Schutzbedarfsziele	DSFA-Zielerfuellungsmanagement_DigiExam_v1.0.xlsx
6	Verzeichnis von Verarbeitungstätigkeiten (VVT)	20210301_Verzeichnis_Verarbeitungstätigkeiten_VVT_v2.3.xlsx
7	Einwilligungserklärung Studierende	Anhangsverzeichnis Punkt 8

2. Kontext

2.1 Überblick

2.1.1 ■Welche Verarbeitung ist geplant?■

Einsatz von DigiExam zur Abnahme von Online-E-Prüfungen

2.1.2 ■Welche Zwecke hat die Verarbeitung?■

Täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation

2.1.3 ■Welche Rechtsgrundlagen/Befugnisse für die Verarbeitung gibt es?■

Für Studierende:

Einwilligung gemäß Art. 9 Abs. 2 lit. a) DSGVO

Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO.

biometrische Gesichtsmerkmale, im Sinne des Art. 9 Abs (1) DSGVO, werden aus Bild extrahiert

Für Mitarbeiter:innen der Hochschule:

Landesbeamtengesetz BW (LBG)

Art. 6 Abs. 1 lit. b) bzw. e), Abs. 3, Art. 88 DS-GVO i.V.m. §§ 12 Absatz 1 S. 1 LHG, 56 LHG § 15 Absatz 1 LDSG und §§ 83 ff.

2.1.4 ■Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?■

Einwilligungserklärung zu Online-E-Prüfungen via E-Mail an Studierendenverteiler (siehe Anlage 7: Unverbindliche_Anmeldung_zur_Online-Pr_fung_20202.pdf)

Einwilligung gemäß Art. 9 Abs. 2 lit. a) DSGVO

Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO.

2.1.5 ■Welche weiteren Normen, Standards und Zertifizierungen gibt es, die für die Verarbeitung relevant sind?■

LHG BaWü, SPO der Hochschule Aalen, Coronasatzung der Hochschule Aalen, GG

2.1.6 ■Welche Zuständigkeiten bestehen für die Verarbeitung?■

Siehe Anlage Nr.6: Verzeichnis von Verarbeitungstätigkeiten (VVT)

2.1.7 ■Wie sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?■

Siehe Anlage Nr. 1

2.1.8 ■ Wurde der Standpunkt der betroffenen Personen eingeholt? ■

2.1.8.1 Wurde der Standpunkt der betroffenen Personen oder ihrer Vertreter eingeholt?

☒ Ja ☐ Nein

2.1.8.2 Anmerkung/Begründung

Gespräch mit VS, Infoveranstaltungen

2.2 Daten, Prozesse und Unterstützung

2.2.1 ■ Welche Kategorien personenbezogener Daten werden verarbeitetet? ■

Siehe Anlage Nr.6: Verzeichnis von Verarbeitungstätigkeiten (VVT)

2.2.2 ■ Welche Kategorien von Personen sind von der Verarbeitung betroffen? ■

Siehe Anlage 6: siehe Anlage Nr.6: Verzeichnis von Verarbeitungstätigkeiten (VVT)

2.2.3 ■ Welche Empfänger, denen die personenbezogenen Daten offengelegt werden, einschließlich Empfänger in Drittländern oder internationale Organisationen gibt es? ■

Nr.	Empfänger	Anlass der Offenlegung	Anmerkung
1	DigiExam Solutions Sweden AB	Anbieter des Dienstes	

2.2.4 ■ Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung? ■

IT-Infrastruktur der Hochschule Aalen

3. Grundlegende Prinzipien

3.1 Verhältnismäßigkeit und Notwendigkeit

3.1.1 **Warum ist die Verarbeitung zwingend erforderlich und ein verhältnismäßiges Mittel, den angestrebten Zweck zu erreichen?**

Täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation, Aufrechterhaltung der Prüfungsphase während der Corona-Krise

3.1.2 **Warum sind die Daten erforderlich?**

Gewährleistung einer täuschungsfreien Durchführung von Online-E-Klausuren

3.1.3 **Wie werden die Daten korrekt und auf dem neuesten Stand gehalten?**

Daten, die aktuell gehalten werden müssen (Benutzerdaten), werden über zentrale Accountverwaltung der Hochschule aktuell gehalten

3.1.4 **Welche Speicherdauer haben die Daten?**

Siehe Anlage Nr.2: Speicherdauer / Löschfristen DigiExam

3.2 Umsetzung der Betroffenenrechte

3.2.1 **Wie werden die betroffenen Personen über die Verarbeitung informiert?**

Siehe Anlage Nr.3: Infoschreiben DigiExam

3.2.2 **Wie können Betroffene ihr Recht auf Auskunft ausüben?**

Formlose Anfrage an die Hochschule Aalen stellen

3.2.3 **Wie können betroffene Personen ihr Recht auf Löschung ausüben?**

Formlose Anfrage an die Hochschule Aalen stellen

3.2.4 **Wie können betroffene Personen ihr Recht auf Berichtigung ausüben?**

Formlose Anfrage an die Hochschule Aalen stellen

3.2.5 **Wie können betroffene Personen ihr Recht auf Einschränkung oder Widerspruch der Verarbeitung ausüben?**

Formlosen Widerspruch an die Hochschule Aalen stellen

3.2.6 Wie können betroffene Personen ihr Recht auf Datenübertragbarkeit ausüben?

Formlose Anfrage an die Hochschule Aalen stellen

4. Risiken

4.1 Risikoanalyse

4.1.1 Wie wird die Erfüllung der SDM-Datensicherheitsziele gewährleistet?

Für die SDM-Gewährleistungsziele der klassischen Informationssicherheit „Verfügbarkeit", „Vertraulichkeit" und den Teilaspekt „Datenintegrität" des SDM-Gewährleistungsziels „Integrität" wurde die Risikoanalyse mittels einer klassischen Risikomanagementmethode ermittelt. Die genaue Durchführung und Ergebnisse sind aus der Anlage 4 „Risikoanalyse Datensicherheitsziele" ersichtlich.

4.1.2 Wie wird die Erfüllung der SDM-Schutzbedarfsziele gewährleistet?

Für die SDM-Gewährleistungsziele „Datenminimierung", „Intervenierbarkeit", „Transparenz" und „Nichtverkettung" sowie der Teilaspekte „Konzepteinhaltung" und „Richtigkeit" des SDM-Gewährleistungsziels „Integrität" wurde die Risikoanalyse anhand eines Zielerfüllungsmanagements durchgeführt, dessen Inhalte und Ergebnisse sich aus der Anlage 5 „Risikoanalyse Schutzbedarfsziele" ergeben.

4.1.3 Risikogesamtbewertung: Wie wird die Einhaltung der DSGVO gewährleistet?

Ergebnis Zielgesamtbewertung:
Die beiden durchgeführten Risikoanalysen (siehe Punkte 4.1.1 und 4.1.2) führten im Hinblick auf die SDM-Gewährleistungszeile zu folgendem Ergebnis:

1.	Verfügbarkeit:	gelb
2.	Vertraulichkeit:	gelb
3.	Datenintegrität:	gelb
4.	Datenminimierung:	grün
5.	Intervenierbarkeit:	gelb
6.	Transparenz:	gelb
7.	Nichtverkettung:	gelb
8.	Konzeptionseinhaltung:	gelb
9.	Richtigkeit:	grün

Die Durchführung der DSFA, einschließlich der Risikoanalyse, erfolgte korrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen. Die Verarbeitungstätigkeit geht unter Umsetzung der technisch-organisatorischen Maßnahmen in die Nutzung über.

4.1.4 ■ Abstimmung mit der zuständigen Aufsichtsbehörde? ■

4.1.4.1 Wurde die zuständige Aufsichtsbehörde konsultiert bzw. ist eine Konsultation geplant?

☐ Ja ☒ Nein

4.1.4.2 Begründung

Keine hohen Restrisiken identifiziert.

4.1.4.3 Beschreibung der Abstimmung (zeitlicher Verlauf, Status, Verweis auf Schriftverkehr, Ergebnisse usw.)

Ausfüllhinweise zum Formular

A) Allgemeines

- Der Begriff „**Daten**“ steht in diesem Formular für „personenbezogene Daten“.
- Der Begriff „**DSFA**“ wird in diesem Formular für „DSFA-Bericht“ verwendet

Glossar

Begriff/Abkürzung	Erläuterung
Daten	Personenbezogene Daten
DSFA	Datenschutz-Folgenabschätzung
SDM	Standard-Datenschutzmodell beschreibt eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Näheres im Internet unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.
SDM-Datensicherheitsziele	Davon umfasst sind die beiden SDM-Gewährleistungsziele Verfügbarkeit und Vertraulichkeit sowie der Teilzielaspekt Datenintegrität des SDM-Gewährleistungsziels Integrität.
SDM-Schutzbedarfsziele	Davon umfasst sind die vier SDM-Gewährleistungsziele Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung sowie der Teilzielaspekt Konzeptionseinhaltung und Richtigkeit des SDM-Gewährleistungsziels Integrität.

Anlage 11: Liste der Unterauftragsverarbeiter (DigiExam)

DigiExam

APPENDIX A
SUBPROCESSORS EU

Data Processing Agreement

Last updated: 2021-01-27

DigiExam Solutions Sweden AB
C/O United Spaces
Torsgatan 26
113 21 Stockholm

DigiExam

Subcontractors

DigiExam use a range of third party subprocessors to provide the service. The data processing agreement between DigiExam and the third party is provided upon request by sending an email to privacy@digiexam.com.

Data processor	Location	Agreements signed	Service provided	Categories of personal data
Elastic	EU	Data Processing Agreement with GDPR Compliance	Search engine that improves the accuracy and speed of search features in DigiExam	Name, email, student code, accessibility settings
Google Cloud Platform	EU	Data Processing Agreement with GDPR Compliance	Cloud service used for hosting the DigiExam platform	All categories that are processed
Kayako	EU	Data Processing Agreement with GDPR Compliance	Platform to manage end-user in-app chats	Name, email
MailJet	EU	Data Processing Agreement with GDPR Compliance	Platform used to send transactional emails	Name, email

Anlage 12: Business Continuity Manual (DigiExam)

DigiExam

BUSINESS CONTINUITY MANUAL

Last updated: 2021-03-05

DigiExam Solutions Sweden AB
C/O United Spaces
Torsgatan 26
113 21 Stockholm

DigiExam

Versions

Version	Date	Author	Description
1.4	2021-03-05	[redacted]	[redacted]
1.3	2020-11-02	[redacted]	[redacted]
1.2	2019-10-28	[redacted]	[redacted]
1.1	2018-10-29	[redacted]	[redacted]
1.0	2018-04-09	[redacted]	[redacted]

Introduction

This document contains instructions on how to act in an exceptional event, either business or disaster. It covers both what is traditionally called Business Continuity Plan and Disaster Recovery Plan.

[redacted]

Key personnel

- [redacted]

Escalation plan

[redacted]

Communication to be done

- [redacted]

Information to be included

- [redacted]

DigiExam

- [redacted]

Scenarios

Unavailable physical premises

[redacted]

- [redacted]

Google Cloud region becomes long term unavailable

[redacted]

- [redacted]

[redacted]

- [redacted]

DigiExam

[redacted]

All of Google Cloud becomes long term unavailable

[redacted]

Single customer loss of data

[redacted]

Key personnel become unavailable

[redacted]

- [redacted]

Disaster close to an office location, man-made (act of terror etc) or natural (hurricane, earthquake etc.)

Perform the following tasks:

- [redacted]

[redacted]