

**Anlage 1: Verzeichnis von Verarbeitungstätigkeiten VVT**

**separat**

**Anlage 2: Auftragsverarbeitungsvertrag AVV**

**DigiExam Solutions Sweden AB**, corporate registration number 556869-1504, Smidesvägen 10, 171 41 Solna, Stockholm, Sweden, hereinafter referred to as “the Supplier”, and

**Aalen University**, corporate registration number. (Steuer-Nr.) 50077 08 203, hereinafter referred to as “the Customer”, has today entered into the following agreement

#### AGREEMENT

#### 1. BACKGROUND AND THE PURPOSE OF THE AGREEMENT

1.1 The Supplier provides a software system for creating, launching, distributing, implementing and evaluating examinations digitally and related Supplementary Services (the “Services”). The Customer wishes the Supplier to provide the Services to the Customer, and the Supplier wishes to provide the Services to the Customer, in accordance with the provisions of this Agreement.

1.2 This Agreement grants the Customer the right to use the software provided by the Supplier in relation to the Service and to obtain access to the Service within a limited time period, further described in Appendix 2, for the fee set out in Appendix 1.

#### 2. DOCUMENTS

2.1 This Agreement consists of this signing page and the following appended documents. If the documents consist of conflicting provisions, the documents of the agreement shall prevail in the following order:

- 1) This Agreement’s Signing Page
- 2) The Data Processing Agreement (including sub processors)
- 3) Appendix 1 – A mutually agreed Proposal.
- 4) Appendix 2 – General Terms and Conditions
- 5) Appendix 3 – Support and Service Level Agreement

#### 3. THE TERM AND TERMINATION OF THE AGREEMENT

3.1 This Agreement shall enter into force upon signing of this Agreement and shall, if the Agreement is not terminated in accordance with the terms of the Agreement, continue to be in force for an initial period of one (1) year and can (option year 2) thereafter be prolonged with one (1) year after a new purchase order from the Customer.

#### 4. CONTACT INFORMATION

Supplier

Customer

Kanzlerin

Telephone: +49 7361 576-

E-mail:

@hs-aalen.de

This Agreement has been signed electronically, of which the parties have received one (1) copy each. The Agreement enters into force on the day both parties have signed the Agreement.

Date: 2020-05-18

Date: 2020-05-18

**DigiExam Solutions Sweden AB**

**Aalen University**

\_\_\_\_\_

Title: Kanzlerin



# **DATA PROCESSING AGREEMENT**

DigiExam Solutions Sweden AB  
Smidesvägen 10  
171 41, Solna, Stockholm  
Sweden

## DATA PROCESSING AGREEMENT

This agreement (the "Agreement") has, upon the signing day, been entered into force by the parties;

**1) Customer:** Aalen University (Hochschule Aalen - Technik und Wirtschaft)  
**Reg No.:** Steuer-Nr. 50077 08 203, VAT-number: DE153480801  
**Address:** Beethovenstraße 1. 73430, Aalen.  
("the Customer" or "the Data Controller") and

**2) Supplier:** DIGIEXAM SOLUTIONS SWEDEN AB,  
**Reg. No.:** 556869-1504,  
**Address:** SMIDESVÄGEN 10, 171 41 SOLNA, STOCKHOLM, SWEDEN  
(the "Supplier" or the "Data Processor").

**Aalen University** and **DigiExam Solutions Sweden AB** are hereinafter individually referred to as the "Party" and collectively as the "Parties".

### 1 DEFINITIONS

- 1.1 Capitalized terms used in this Agreement but not otherwise defined in this Agreement shall have the meanings assigned to them under the GDPR (in particular under its Article 4 ("Definitions")).
- 1.2 "EEA" means European Economic Area, which consists of the EU member states plus Iceland, Liechtenstein and Norway.
- 1.3 "Data Protection Legislation" means the regulatory framework regarding data protection applicable to the Controller and the Processor, in particular the GDPR. The Data protection legislation also covers national law regulating the Processing of Personal Data, including precedents and the supervisory authorities' regulations and recommendations regarding data protection.
- 1.4 "GDPR" means the Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- 1.5 This Agreement is applied, interpreted and has equivalent definitions to those provided in the GDPR and any applicable Data Protection Legislation.

## **2 CONTENTS AND PURPOSE**

- 2.1 The Supplier and the Customer have entered into the agreement "DigiExam – Aalen University – SaaS Agreement" (the "Main Agreement"). According to the Main Agreement, the Customer has commissioned the Supplier to deliver certain IT-services for conducting examinations digitally. Such services are further defined in the Main Agreement. The Supplier will in respect of the cooperation with the Customer process Personal Data on behalf of the Customer.
- 2.2 The purpose of this Agreement is to fulfil the requirements of an agreement between the Customer as the Data Controller and the Supplier as the Data Processor.
- 2.3 The Agreement shall take precedence over the provisions concerning Personal Data processing in the Main Agreement, unless otherwise stated in writing.

## **3 RESPONSIBILITY AND INSTRUCTION**

- 3.1 The Data Processor undertakes to only process Personal Data in accordance with this Agreement, the Main Agreement, applicable Data Protection Legislation, and the Data Controller's written instructions and only to the extent necessary for the performance of the Main Agreement. In case of inconsistencies, this Agreement shall take precedence over any other previously given instructions, unless otherwise has been agreed upon between the Parties.
- 3.2 The Data Controller is responsible for all Processing of Personal Data by the Data Processor on behalf of the Data Controller in order meet the requirements under the Main Agreement.
- 3.3 This Agreement and the Main Agreement shall form the basis of the Data Controller's instructions. The instructions include, but are not limited to, the following:

(i) General nature and purpose of the Processing:

The Processor processes Personal Data for the purpose of providing the services as stated in the Main Agreement.

(ii) Categories of Data Subjects:

- Controller employees, other staff and representatives
- Students

(iii) Categories of Personal Data:

- Personal identification number, name, surname,

- E-mail

- Device information (IP-address, MAC address, domain addresses, computer operating system, geolocation data)

- Employment information (job title, function, name of employer)

(IV) Duration of the data processing

The Personal Data will be processed as long as the Main Agreement is in force.

(V)

Deletion of Personal Data is done upon request from Data Controller.

Personal Data will be deleted from the primary database upon received notice from Data Controller and be entirely deleted within 180 days after received and acknowledged notice from Data Controller.

- 3.4 The Data Processor shall maintain a record of processing activities carried out by the Data Processor or its sub-processors, including the categories of Personal Data in accordance with, at any time current and applicable Data Protection Legislation.
- 3.5 The Data Processor shall make sure that all employees, consultants and other persons which the Data Processor is responsible for, and who are processing the Personal Data, shall be informed of how the processing shall be carried out.
- 3.6 The Data Processor shall assist the Data Controller with the implementation of appropriate technical and organizational measures in such a manner that the Data Controller fulfills its requirements towards the Data Subjects in accordance with any from time to time applicable Data Protection Legislation, in particular Chapter III in the GDPR.
- 3.7 The Data Controller is responsible for giving the Data Processor adequate instructions in order for the parties to be able to fulfill the applicable requirements regarding the processing of the Personal Data.
- 3.8 The Data Processor shall assist the Data Controller in order to ensure that the obligations in relation to a Data Breach can be adhered to according to Articles 33-34 in the GDPR. The Data Processor shall notify the Data Controller without undue delay after becoming aware of a Personal Data breach or similar incidents. The notification shall at least:
- (i) describe the nature of the Personal Data breach including the categories and approximate number of data subjects and Personal Data records concerned,
  - (ii) communicate the name and contact details of the data protection officer or other contacts where further information can be obtained,



- (iii) describe the likely consequences of the Personal Data breach,
  - (iv) describe the measures taken or proposed to be taken by the Data Processor to address the Personal Data breach, including, measures to mitigate its possible adverse effects.
- 3.9 Where it is not possible for the Data Processor to provide the information as indicated in Section 3.8 at the same time, the information may be provided in phases without undue further delay, which also applies in case the Data Controller requests additional information from the Data Processor.
- 3.10 The Data Processor shall, upon request, give the Data Controller access to all information necessary to show that the Data Processor's obligations under the Agreement have been fulfilled. The Data Processor shall also allow and facilitate the reviews, including inspections, that the Data Controller, accountant, supervisory authority or any other affected party, according to the applicable Data Protection Legislation or the Agreement and the Main Agreement may require ("Inspections").
- 3.11 The Data Processor shall assist the Data Controller in accordance with applicable Data Protection Legislation, in particular Articles 35-36 in the GDPR, and recommendations of the supervisory authorities in case the Data Controller conducts a data protection impact assessment of the consequences for the protection of the Personal Data of the planned processing and/or any prior consultation with any supervisory authority. The Data Processor is entitled to reasonable remuneration for this.
- 3.12 The Data Processor shall make sure that the Personal Data is deleted or returned in accordance with the written instructions of the Data Controller, for which the Data Processor is entitled to reasonable remuneration.

#### **4 CONFIDENTIALITY**

- 4.1 Each Party undertakes not to, without the other Party's prior written consent, disclose or reveal to any third parties Personal Data or information about the other Party's business that is reasonably deemed to be regarded as commercial and professional secrets, and hence confidential information. Information which a Party has stated to be confidential is always considered as commercial and professional secrets. The confidentiality requirement does not apply to information which a Party can prove has come to its knowledge outside the assignment or which is public knowledge. The confidentiality requirement also does not apply when a Party is required by law to disclose information.
- 4.2 Each Party shall, through confidentiality undertakings or other appropriate measures, ensure that its personnel complies with the confidentiality requirements above. A Party is also responsible for ensuring that its subcontractors and their employees that process

Personal Data sign a confidentiality undertaking not less protective to the other Party, and that such persons only have access to information to the extent which is necessary to complete the assignment.

- 4.3 Notwithstanding the above, the confidentiality provisions of the Main Agreement shall apply to the extent it contains stricter and more extensive confidentiality requirements for each Party compared to the Agreement.
- 4.4 Notwithstanding what is otherwise stated in this Agreement, Section 4 shall survive in case the Agreement is terminated.

## **5 SECURITY**

- 5.1 The Data Processor shall implement appropriate technical and organizational measures in such a manner that the Personal Data is protected by an adequate security level according to Article 32 in the GDPR. This includes, when appropriate:
- (i) the pseudonymisation and encryption of Personal Data,
  - (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
  - (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident,
  - (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- 5.2 In assessing the appropriate level of security according to Section 5.1, account shall particularly be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
- 5.3 The Data Processor shall keep the Data Controller informed of any Inspections in accordance with this Agreement and provide the Data Controller with information about such Inspections and an opportunity to comment on the information that the Data Processor is requested to disclose in relation to the Inspection.
- 5.4 If the Data Processor is imposed costs in order adhere to requirements of security in addition to those explicitly stated in this Agreement or the Main Agreement, the Data Processor is entitled to remuneration from the Data Controller for these costs.

- 5.5 The Data Processor shall, to a reasonable extent, assist in and allow such Inspections which the Data Controller, supervisory authority or other concerned party can request according to applicable Data Protection Legislation or the Agreement for the maintenance of a correct processing of Personal Data. The Data Controller is entitled to remuneration for this.
- 5.6 The Data Processor must comply with decisions taken by supervisory authorities in respect to the processed Personal Data and the technical and organizational measures to protect them.

## **6 OBLIGATIONS AFTER THE TERMINATION OF THE AGREEMENT**

- 6.1 The Parties agree that the Data Processor, in connection with the termination of the data processing, and depending on what the Data Controller decides, either must return the transferred Personal Data and any copies thereof to the Data Controller, and/or to delete all Personal Data and give the Data Controller notice of such deletion.
- 6.2 In cases where the Data Processor is required by applicable Data Protection Legislation to store Personal Data, such requirement will supersede Section 6.1.

## **7 SUB-PROCESSORS**

- 7.1 The Data Processor has the right to engage sub-processors for the processing of the Personal Data on behalf of the Data Controller after the Data Controller's prior written approval. The Data Processor shall inform the Data Controller on any plans to engage new, or replace current sub-processors in order for the Data Controller to be able to object to such changes.
- 7.2 If the Data Processor engages a sub-processor in accordance with the provisions of the Agreement, the Data Processor is authorized and has an obligation to enter into a sub-processing agreement with that sub-processor. The sub-processor shall have the same obligations and liabilities as the Data Processor has according to this Agreement, including but not limited to the security and confidentiality requirements. The Data Processor is liable for the engaged sub-processors as for its own performance. The Data Processor shall, upon the Data Controller's request, provide the relevant parts of any sub-contractor's contract in order to show the compliance with this Agreement.
- 7.3 The Data Processor must at all times keep an adequate and updated register of engaged sub-processors and where they are geographically located. Furthermore, the Data Processor must at the request of the Data Controller, without undue delay, provide the sub-processors' contact information.

## **8 AUDIT AND SUPERVISION**

- 8.1 The Data Controller has the right to, on its own or through a third party, within reasonable extent, undertake an audit of the Data Processor, or in any other way supervise that the Data Processor's data processing of the Personal Data complies with this Agreement. At such an audit or supervision, the Data Processor must be notified in due time and must provide the Data Controller with necessary assistance in order to conduct the audit and the Data Processor shall have right to reasonable compensation thereof.
- 8.2 The Data Processor must upon the Data Controller's request, within reasonable extent, provide available information with respect to the data processing of the Personal Data, in order for the Data Controller to comply with its requirements in accordance with the Agreement or applicable Data Protection Legislation. The Data Processor shall have right to reasonable compensation thereof.
- 8.3 In the event of a request by Data Subjects, supervisory authorities, or any other third party, regarding the data processing of the Personal Data, the Parties shall cooperate and exchange information to a necessary extent. No Party may disclose Personal Data or information about data processing without the other Party's prior consent.

## **9 TRANSFERS TO THIRD COUNTRIES**

- 9.1 The Data Processor undertakes not to transfer the Personal Data outside of the EU/EEA unless done in accordance with application. The Data Processor shall ensure appropriate safeguard measures according to Chapter V in the GDPR.
- 9.2 As part of the Data Processors fulfilment of delivering the Service put forth in the Agreement, Personal Data in relation to support cases and Personal Data used for contact, such as Name phone number and e-mail addresses related to the Data Controllers employees and students might be subject for data processing by the Data Processors Sub-processors specified in Appendix "Subcontractors"

## **10 DISPUTE**

- 10.1 Any disputes in regard to the interpretation or application of this Agreement will be determined according to the Main Agreement's provisions of disputes and applicable law.

## **11 TERM AND TERMINATION**

- 11.1 This Agreement remains in effect as long as the Main Agreement is in force and is deemed as terminated in the event that the Main Agreement is terminated.



11.2 Amendments to the Agreement may be done by mutual written agreements.

11.3 If the Data Processor receives objections from the Data Controller regarding changes of Sub-processors or otherwise receives instructions or demands from the Data Controller, not covered by this Agreement, the Processor shall be entitled to, in its own discretion:

- (i) renegotiate the compensation under the Main Agreement; or
- (ii) without any liability for damages or other liabilities, terminate both the Main Agreement and this Agreement within ninety (90) days from receiving instructions

11.4. Termination section 11.3 above will take effect in connection with the instructions or demands are applicable of/by the Data Controller, or at the time which the Parties otherwise agree upon in writing.



# **DATA PROCESSING AGREEMENT SUBPROCESSORS**

Data Processing Agreement

Last updated: 2019-10-28

*DigiExam AB  
Smidesvägen 10, vån 3  
171 41, Solna  
Sweden*



## Subcontractors

DigiExam use a range of third party subprocessors to provide our service. The signed data processing agreement between DigiExam and the third party is provided upon request by sending an email to [privacy@digixam.com](mailto:privacy@digixam.com).

<b>Data processor</b>	<b>Location</b>	<b>Agreements signed</b>	<b>Service provided</b>	<b>Categories of personal data</b>
Google Cloud Platform	EU	Data Processing Agreement with Privacy Shield and GDPR Compliance	Cloud service for running the platform	All categories that are processed
ZenDesk	US	Data Processing Agreement with Privacy Shield and GDPR Compliance	Platform to manage end-user support requests	Name, email
Intercom	US	Data Processing Agreement with Privacy Shield and GDPR Compliance	Platform to manage end-user in-app chats	Name, email
SendGrid	US	Data Processing Agreement with Privacy Shield and GDPR Compliance	Platform to send transactional emails	Name, email
MailChimp	US	Data Processing Agreement with Privacy Shield and GDPR Compliance	Platform to send promotional emails	Name, email



## APPENDIX 3 - SUPPORT AND SERVICE LEVEL AGREEMENT

THIS DIGIEXAM SERVICE LEVEL AGREEMENT ("SLA") between DigiExam Solutions Sweden AB. ("DigiExam", "us" or "we") and users of the DigiExam Services ("you") governs the use of the DigiExam Services under the provisions of the DigiExam Service Agreement.

Unless otherwise provided herein, this SLA is subject to the provisions of the Service Agreement.

### 1. Service Commitment

DigiExam will use commercially reasonable efforts to make your DigiExam Services running in dedicated environments available with an Uptime Percentage of at least 99.9% during any billing cycle. Subject to the SLA Exclusions, if we do not meet the Service Commitment, you will be eligible to receive a Service Credit.

### 2. Definitions

(a) *Maintenance.* Scheduled Unavailability of the DigiExam Services, as announced by us prior to the DigiExam Services becoming Unavailable.

(b) *Uptime Percentage.* Calculated by subtracting from 100% the percentage of minutes during the billing cycle in which the DigiExam Services were Unavailable. Uptime Percentage measurements exclude downtime resulting directly or indirectly from any SLA Exclusion.

(c) *Service Credit.* A credit denominated in EUR €, calculated as set forth below, that we may credit back to an eligible account.

(d) *Unavailable. / Unavailability.* Mean, for app services and databases, when your service or database is not running or not reachable due to DigiExam's fault.

### 3. Commitments and Service Credits

Service Credits are calculated as a percentage of the total charges due on your DigiExam invoice for the billing cycle in which the Unavailability occurred, applied proportionally to the Services that were Unavailable, in accordance with the schedule below:

(a) For Uptime Percentage, less than 99.9% but equal to or greater than 99.0%, you will be eligible for a Service Credit of 10% of the charges attributable to the affected resources



- (b) For Uptime Percentage less than 99.0%, you will be eligible for a Service Credit of 30% of the charges attributable to the affected resources

We will apply any Service Credits only against future payments for the Services otherwise due from you. Service Credits will not entitle you to any refund or other payment from DigiExam. A Service Credit will be applicable and issued only if the credit amount for the applicable billing cycle is greater than 100 EUR (€100). Service Credits may not be transferred or applied to any other account.

#### **4. Sole Remedy**

Unless otherwise provided in the Service Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Services is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

#### **5. Credit Request and Payment Procedures**

To receive a Service Credit, you must submit a claim by emailing support@digixam.com. To be eligible, the credit request must be received by us by the end of the billing cycle after which the incident occurred and must include:

- (a) the words "SLA Credit Request" in the subject line;
- (b) the dates and times of each Unavailability incident that you are claiming;
- (c) the account handle(s); and
- (d) logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).
- (e) If the Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

#### **6. SLA Exclusions**

The Service Commitment does not apply to any Unavailability:

- (a) Caused by factors outside of our reasonable control, including any force majeure event, Internet access, or problems beyond the demarcation point of the DigiExam services;
- (b) That results from any actions or inactions of you or any third party;

(c) That results from the equipment, software or other technology of you or any third party (other than third party equipment within our direct control);

(d) That results from any Maintenance.

If availability is impacted by factors other than those used in our Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

## **7. Support**

Support regarding technical questions, bug fixes and non-urgent issues is primarily handled through the DigiExam online support which is integrated in the DigiExam platform to enable you to get fast and structured feedback. The online support is free and included for all Customers. The online support does not include questions regarding training, workshops or demos.

You may also call us in case of emergency situations. With emergency situations we mean issues that the administrator-/s or the account manager at the school cannot handle themselves during an examination process despite the information and instructions in manuals, videos or guides.

All support is handled during normal office hours\* if nothing else has been decided in the Main Agreement or if support outside of normal office hours has been ordered as a separate service.

Response time:

- 0-3 hours (during normal office hours) for support errands with urgent priority
- 0-8 hours (during normal office hours) for support errands with high priority
- Within 24 hours (during normal office hours) for support errands with normal priority
- Within 48 hours (during normal office hours) for support errands with low priority

\*Normal office hours are Monday-Friday 8am - 5pm CET (GMT +1) / CEST (GMT +2), except Swedish public holidays.

E-mail: [support@digixam.com](mailto:support@digixam.com)

### **Priority framework**

Description of incident types and how they are prioritized and assigned:

#### **Urgent priority**

##### **Description**

This is an emergency condition that restricts the use of the service so that mission critical business functions cannot be used as intended or are unavailable for multiple people.

Only support errands of critical severity level according to the "Overall Risk Severity" table in [QWASP Risk Rating Methodology](#) will be given an urgent priority.

##### **Response time**

Within 0-3 hours of receiving notification with a follow-up phone call, voice mail and/or e-mail.

#### **Resolution time**

The resolution target time is 8 hours for urgent incidents and the incident will be handled as urgent until the incident has been resolved or a workaround exists.

#### **Status updates**

A status update will be provided within 2 hours of the follow-up. For urgent incidents, status updates will be provided continuously until a resolution or workaround can be found.

#### **Request examples**

a) The DigiExam web application freezes immediately upon login, crashes upon login or is unavailable for multiple people.

b) Data disappears or becomes unusable/corrupted for multiple people.

Example 1: Data is not saved when grading exams.

Example 2: Data is not saved/submitted when students hand in exams.

c) Mission critical business functions are unavailable for multiple people.

Example 1: Student client crash on start up after new release.

Example 2: Teachers can't start exams.

#### **High priority**

##### **Description**

DigiExam is up and running but in a restricted or limited state due to key features being unavailable with no acceptable workaround or DigiExam can't be used due to unstable availability.

Only support errands of high severity level according to the "Overall Risk Severity" table in OWASP Risk Rating Methodology will be given a high priority.

##### **Response time**

Within 0-8 hours of receiving notification with a follow-up through phone call, voice mail and/or e-mail.

##### **Resolution time**

The resolution target time is 16 hours for high priority incidents and the incident will be handled as high priority until the incident has been resolved or a workaround exists.

##### **Status updates**

For high priority incidents status updates will be provided on a daily basis until a resolution or workaround can be found.

##### **Request Examples**

a) DigiExam web application stops working in frequent recurring intervals for multiple people

which forces the user to log out and then login again in order to continue working.

Example: DigiExam web application freezes after each time an exam is saved while editing it.

b) Major performance issues for multiple people that make it difficult or impossible to work with DigiExam.

Example: All views in the DigiExam web application take 5 minutes or more to load when switching between views. **Note** that if a single view loads slowly it is a minor performance issue which can be found under low priority.

c) DigiExam can be used, but in a limited state due to key features being unavailable for multiple people.

Example: The monitoring view doesn't present any data in the DigiExam web application.

### **Normal priority**

#### **Description**

DigiExam is up and running but in a restricted or limited state due to key features being unavailable but with an acceptable workaround.

Only support errands of medium severity level according to the "Overall Risk Severity" table in OWASP Risk Rating Methodology will be given a normal priority.

#### **Response time**

Within 24 hours.

#### **Resolution time**

The resolution target time is 40 hours (5 business days) for normal priority incidents. An incident is considered resolved when an acceptable workaround has been reached, full resolution to the problem will be implemented earliest in the next planned release.

#### **Status updates**

For normal priority incidents status update will be provided upon incident resolution.

#### **Request examples**

a) Error messages that have acceptable workarounds.

Example: The student search produces an error message when trying to find and enable spell check for a specific student. As an acceptable workaround, the teacher can use the accessibility settings during the exam to give a specific student the ability to use spell check.

b) DigiExam key features don't work as intended but have acceptable workaround.

Example: The monitoring view is only updated on student exam start and hand in, but not continuously during the exam.

### **Low priority**

#### **Description**

Minor issues that don't affect any key features, secondary features are unavailable but can easily be worked around or avoided. Feedback, feature requests or general questions that can be

answered by FAQ or through documentation. These issues or questions don't impact the customer's use of DigiExam to the extent that issues with higher priority do.

Only support errands of low severity level according to the "Overall Risk Severity" table in [QWASP Risk Rating Methodology](#) will be given a low priority.

**Response time**

Within 48 hours

**Resolution time**

The resolution target time is 80 hours (10 business days) for low priority incidents. An incident is considered resolved when an acceptable workaround has been reached, full resolution to the problem will be implemented earliest in the next planned release.

**Status updates**

For low priority incidents status update will be provided upon incident resolution.

**Request examples**

a) DigiExam secondary features don't work as intended but have acceptable workaround.  
Example: Spreadsheet export feature is unavailable, as a workaround the teacher can copy/paste student results manually from the grades view.

b) Minor performance issues.

Example 1: Exam hand ins take longer than usual as a student.

Example 2: Monitoring view takes longer than usual to load in student data.

c) General questions on how to use DigiExam.

Example 1: Information regarding where the spell check feature can be found and how it's used.

Example 2: Information regarding how to create, start, end exam.

d) Clarification of documentation or user guides.

Example: Information regarding how to do an LTI integration for a specific LMS.

### **Anlage 3: Technische und organisatorische Maßnahmen TOMs**

**Technische und organisatorische Maßnahmen der Hochschule Aalen zum sicheren Betrieb der IT-Systeme**

Nr.	Kontrollziele	Maßnahmen
1	<p><b>Zutrittskontrolle</b> (Räume und Gebäude)</p> <p><u>Zielbeschreibung:</u> Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren.</p>	<p>Die Dienstleistung wird als Software-as-a-Service (SaaS) von der Firma DigiExam Solutions AB genutzt. Zugang zur Software erhält die Hochschule über <a href="https://app.digiexam.com/app#/">https://app.digiexam.com/app#/</a>.</p> <p>Der Dienstleister hat sich vertraglich dazu verpflichtet, die erforderlichen Maßnahmen zwecks Zutrittskontrolle zu treffen. Die Dokumentation zu technischen und organisatorischen Maßnahmen des Dienstleisters ist anbei (s. Anlage 13).</p>
2	<p><b>Datenträgerkontrolle</b> (Physikalische und elektronische Datenträger)</p> <p><u>Zielbeschreibung:</u> Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.</p>	<p>Die Dienstleistung wird als Software-as-a-Service (SaaS) von der Firma DigiExam Solutions AB genutzt. Zugang zur Software erhält die Hochschule über <a href="https://app.digiexam.com/app#/">https://app.digiexam.com/app#/</a>. Der Dienstleister hat sich vertraglich dazu verpflichtet, die erforderlichen Maßnahmen zwecks Datenträgerkontrolle zu treffen. Die Dokumentation zu technischen und organisatorischen Maßnahmen des Dienstleisters ist anbei (s. Anlage 13). Physikalische Datenträger werden in der EU aufbewahrt. Der Datenverarbeiter seitens DigiExam muss über ein aktuelles Verzeichnis der Standorte verfügen.</p> <p>Elektronische Datenträger werden weltweit aufbewahrt und die Standorte werden von dem Datenverarbeiter seitens DigiExam dokumentiert. Die Datenverarbeiter werden im Dokument Anlage 11 aufgezählt.</p>
3	<p><b>Speicherkontrolle</b> (IT-System, Datenträger)</p> <p><u>Zielbeschreibung:</u> Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern.</p>	<p>Die Dienstleistung wird als Software-as-a-Service (SaaS) von der Firma DigiExam Solutions AB genutzt. Zugang zur Software erhält die Hochschule über <a href="https://app.digiexam.com/app#/">https://app.digiexam.com/app#/</a>. Der Dienstleister hat sich vertraglich dazu verpflichtet, die erforderlichen Maßnahmen zwecks Speicherkontrolle zu treffen. Die Dokumentation zu technischen und organisatorischen Maßnahmen des Dienstleisters ist anbei (s. Anlage 13). Jeder Eingriff in die persönlichen Daten wird nur durch eine Genehmigung des Dienstleisters ermöglicht. Eine limitierte Anzahl an Personen haben Zugriff darauf.</p> <p>Mehr Informationen sind im Dokument Anlage 2 und Anlage 13 zu finden.</p>
4	<p><b>Benutzerkontrolle</b> (IT-Systeme, Anwendungen)</p> <p><u>Zielbeschreibung:</u> Es ist zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.</p>	<p>Für Administratoren:</p> <p>Ein dezidiertes Rollen- und Berechtigungskonzept legen die nutzungsberechtigten Personen fest. Für jede Fakultät werden Administratoren bestimmt. Die Berechtigungsstruktur wird im Learning Management gepflegt und ist ebenfalls mit der zentralen Accountverwaltung der Hochschule gekoppelt, wodurch Berechtigungen beim Ausscheiden automatisch entzogen werden. Die Berechtigungsstruktur in DigiExam wird weiter mit dem LMS synchronisiert, dadurch bleiben die Berechtigungen ebenfalls auf dem neusten Stand.</p>



		<p>Für Dozierende:</p> <p>Für Dozierende wird ebenfalls die Berechtigungsstruktur aus dem LMS übernommen, wodurch Zugriff auf die eigens erstellten Prüfungsinhalte gewährt wird.</p> <p>Für Studierende:</p> <p>Studierende nutzen für die Durchführungen der Prüfungen auf DigiExam einen Client. Der Client wird dem den Studierenden auf der DigiExam Homepage zur Verfügung gestellt. Die Anmeldung von der Registrierung erfolgt wiederum über das LMS.</p> <p>Ein Rollenkonzept ist im Dokument Anlage 5 beschrieben.</p>
5	<p><b>Zugriffskontrolle</b> (Auf Daten)</p> <p><u>Zielbeschreibung:</u> Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.</p>	<p>Der Zugang wird über das Learning Management System (LMS) Canvas der Firma Instructure über eine Schnittstelle (LTI) ermöglicht. Dadurch ist der Zugang implizit auch über die Authentifizierung der Hochschule geregelt. Durch Single-Sign on wird der Zugriff gewährleistet. Der Zugriff ist passwortgeschützt und das Passwort kann nur im Hochschul-Netzwerk geändert werden. Es gelten folgende Vorgaben für die Passwortkomplexität: Ein gültiges Passwort muss mindestens 10 Zeichen haben, Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen enthalten. Auch darf es keine zu große Ähnlichkeit mit dem aktuellen Passwort haben. Mit der Sperrung des Zugangs zu Canvas wird somit auch der Zugang über die Schnittstelle (LTI) gesperrt.</p> <p>Durch das eingesetzte Rollenkonzept wird nur die notwendige Berechtigung für den jeweiligen Bereich gewährt. Die Erstellung von „Log data“ erfolgt nur, sofern sie tatsächlich erforderlich sind, bspw. notwendig für die Fehlerbehebung durch den Dienstleister. Personenbezogene Log Daten werden bis zu 180 Tagen gespeichert. (vergleiche Anhang 14)</p>
6	<p><b>Übermittlungskontrolle</b></p> <p><u>Zielbeschreibung:</u> Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.</p>	<p>Die Übermittlung zurück an Canvas wird über die LTI -Schnittstelle gesteuert. Weitere Systeme sind nicht angebunden.</p>
7	<p><b>Eingabekontrolle</b> (in Datenverarbeitungssysteme)</p> <p><u>Zielbeschreibung:</u> Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu</p>	<p>Die Dienstleistung wird als Software-as-a-Service (SaaS) von der Firma DigiExam Solutions AB genutzt. Zugang zur Software erhält die Hochschule über <a href="https://app.digiexam.com/app#/">https://app.digiexam.com/app#/</a>. Der Dienstleister hat sich vertraglich dazu verpflichtet, die erforderlichen Maßnahmen zwecks Eingabekontrolle zu treffen. Die Dokumentation zu technischen und organisatorischen Maßnahmen des Dienstleisters ist anbei (s. Anlage 13, 9.5.2 Audit logs). Die Uhrzeit, die Instanz sowie das Ereignis werden durch „Log Data“ protokolliert und können genauestens nachverfolgt werden. Die</p>





	welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.	<p>Logdatei erhält einen eindeutigen Namen, aus dem die Protokollespeichernde Instanz und der Zeitraum der Log-Datenerfassungen hervorgehen. In der Regel werden Protokolldaten nur zu den Zwecken, die Anlass für ihre Speicherung waren, ausgewertet werden. Über diese Zwecke wurden Beschäftigte aufgeklärt werden. Um durchgehend feststellen zu können, ob die Zweckbindung eingehalten wird, werden Protokolldaten unterschiedlicher Ebenen (Prüfer, IT-Infrastruktur, Administration) miteinander in eine Beziehung gesetzt, um die Rechtskonformität aller Aktivitäten auf den verschiedenen Ebenen nachweisen zu können.</p> <p>Weiter Informationen ist hier, unter der Rubrik „Data Collected Automatically“ zu entnehmen:  <a href="https://storage.googleapis.com/digixam/about/privacy_policy_eu.pdf">https://storage.googleapis.com/digixam/about/privacy_policy_eu.pdf</a></p>
8	<p><b>Auftragskontrolle</b></p> <p><u>Zielbeschreibung:</u>          Es ist zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.</p>	<p>Es besteht ein Vertrag zur Auftragsdatenverarbeitung mit dem Dienstleister DigiExam Solutions AB. Ohne eine gegenseitige und schriftliche Zustimmung dürfen keine Daten veröffentlicht werden. Die Auswahl des Auftragnehmers erfolgte mit gebotener Sorgfalt (Durchsicht von TOMs des Auftragnehmers, Auswertung der Presseberichte, Auswahl unter europäischen Anbietern etc.). Die Datenlöschung wird überprüft. Die Anweisungen an den Auftragnehmer erfolgen schriftlich. Die Mitarbeiter des Auftragnehmers werden auf Datengeheimnis verpflichtet. Der Auftragnehmer und sein Schutzniveau werden dauerhaft überprüft. Einmal im Quartal findet ein gemeinsamer Termin zwecks Besprechung von einzelnen datenschutzrechtlichen Fragen statt.</p>
9	<p><b>Transportkontrolle</b></p> <p><u>Zielbeschreibung:</u>          Es ist zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.</p>	<p>Die Kommunikation zu den Servern von DigiExam Solutions AB wird grundsätzlich TLS verschlüsselt.</p> <p><a href="https://storage.googleapis.com/digixam/about/privacy_policy_eu.pdf">https://storage.googleapis.com/digixam/about/privacy_policy_eu.pdf</a></p>
10	<p><b>Verfügbarkeitskontrolle</b></p> <p><u>Zielbeschreibung:</u>          Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.</p>	<p>Die Dienstleistung wird als Software-as-a-Service (SaaS) von der Firma DigiExam Solutions AB genutzt. Zugang zur Software erhält die Hochschule über <a href="https://app.digixam.com/app#/">https://app.digixam.com/app#/</a>. Die Dokumentation zu technischen und organisatorischen Maßnahmen des Dienstleisters ist anbei (s. Anlage 13). Nähere Informationen sind ferner im Dokument Anlage 2 unter Punkt 5 zu finden.</p>
11	<p><b>Organisationskontrolle</b></p> <p><u>Zielbeschreibung:</u>          Die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen</p>	<p>Es gilt die Nutzungsrichtlinie (siehe Anlage 6). Es gilt das sog. Vier-Augen-Prinzip für das Verlängern der Löschrufen. Die interne Datenschutzbeauftragte wird bei den Entscheidungen eingebunden. Die für die Verarbeitung von personenbezogenen Daten zuständigen Beschäftigten werden regelmäßig geschult (jährlich). Sie unterschrieben eine Verpflichtungserklärung auf das Datengeheimnis.</p>



	<p>des Datenschutzes gerecht wird.</p>	<p>Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wurde eingeführt (Verantwortliche: Beauftragt ist das Compliance-Team des Canvas-Kernteam in Kooperation der Datenschutzbeauftragten und Stabstelle Datenschutz der Hochschule Aalen). Die Überprüfung erfolgt jährlich. Die Qualität der technischen und organisatorischen Maßnahmen wird in regelmäßigen Abständen getestet. Es finden wöchentliche Treffen mit den Fakultätsadministratoren zu personellen Veränderungen um Berechtigungen zu überprüfen, statt. Ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.</p> <p>Seitens DigiExam siehe Anlage 13, Punkt 8: Human Resources</p>
12	<p><b>Löschen</b></p> <p><u>Zielbeschreibung:</u> Gewährleisten, dass die personenbezogenen Daten nach der Zweckerreichung automatisch und vollständig gelöscht werden.</p>	<p>Besteht kein Täuschungsverdacht, so werden die Aufzeichnungen innerhalb von 2 Wochen nach der Abgabe der Prüfungsleistung von dem Auftragsverarbeiter automatisch gelöscht.</p> <p>Im Verdachtsfall werden die Daten auf Weisung der Hochschule innerhalb von 4 Wochen oder maximal bis zur Klärung des Vorfalls unverzüglich nach der Aufklärung des Sachverhalts gelöscht.</p> <p>Für die Prüfung, Anordnung und Durchführung von Löschungen sind das Compliance-Team des Canvas-Kernteam (und Position bei DigiExam) zuständig.</p> <p>Um die Löschpflichten für die Datenbestände bei Auftragsverarbeiter umsetzen zu können, wurden vertragliche Regelungen getroffen.</p> <p>Das Löschen wird vom Auftragsverarbeiter protokolliert. In diesen Protokollen sind keine Daten enthalten, für die eine Löschverpflichtung besteht.</p>

**Anlage 4: Löschfristen (als Teil der TOMs)**

**separat**

**Anlage 5: Rollenverteilung (als Teil der TOMs)**

Berechtigungen	Admin	Account Manager	Dozent	Student	Aufsicht
Prüfungen anzeigen	✓	x	x	x	x
Klassen anzeigen	✓	x	x	x	x
Kurse anzeigen	✓	x	x	x	x
Abgeschlossen Prüfungen anzeigen	✓	x	x	x	x
Abgeschlossen Klassen anzeigen	✓	x	x	x	x
abgeschlossen Kurse anzeigen	✓	x	x	x	x
Anonymisierung entfernen	✓	x	x	x	x
Suche nach registrierten Studenten / Dozenten	✓	x	x	x	x
Verwalten aller Konten	x	✓	x	x	x
Einladen neuer Dozenten	x	✓	x	x	x
Einladen neuer Studenten	x	✓	x	x	x
Einladen neuer Admins	x	✓	x	x	x
Einladen neuer Account Manager	x	✓	x	x	x
Benutzerzugriff widerrufen	x	✓	x	x	x
Erstellen einer Prüfung	✓	x	✓	x	x
Starten einer Prüfung	✓	x	✓	x	x
Benoten einer Prüfung	✓	x	✓	x	x
Veröffentlichen Prüfungsergebnisse	✓	x	✓	x	x
Feedback auf Studentenaccount	✓	x	✓	x	x
Einsicht ob Prüfung begonnen oder schon abgegeben	✓	x	✓	x	x
Prüfung freischalten	✓	x	✓	x	x
Nach registrierten Studenten suchen	✓	x	✓	x	x
Zugang zur Prüfung	✓	x	✓	✓	x
Überprüfung der Ergebnisse und Rückmeldung die an den Studenten gesendet wurden	✓	x	✓	✓	x
Überwachung einer Prüfung	✓	x	✓	x	✓
Starten einer Prüfung	✓	x	✓	x	✓
Beenden einer Prüfung	✓	x	✓	x	✓
Sperren einer Prüfung	✓	x	✓	x	✓
Entsperren einer Prüfung	✓	x	✓	x	✓

**Anlage 6: Nutzungsrichtlinie DigiExam**

## Nutzungsrichtlinie zu „DigiExam“ an der Hochschule Aalen

DigiExam ist eine Online-Prüfungsumgebung der Firma DigiExam Solutions Sweden AB, die ihren Sitz in Schweden hat.

- Der Dienst darf nur zum Zweck der Prüfungsabnahme und Sicherstellung von Täuschungsfreiheit in einer Prüfung genutzt werden.
- Dritten darf kein Zugriff oder Einsicht in das System gewährt werden, soweit diese nicht mit am Prüfungsverfahren beteiligt sind.
- Ebenso haben die Nutzer\*innen dafür Sorge zu tragen, dass das System nicht von Dritten unzulässigerweise genutzt wird.
- Daten dürfen weder aus dem System exportiert noch anderweitig gespeichert werden. Ausgenommen sind die niedergeschriebenen Prüfungsinhalte für Einsichtszwecke oder zur Korrektur. Diese Daten sind nach Erlöschen des Zwecks unverzüglich zu löschen.
- Wird eine Fehlfunktion des Systems oder eine missbräuchliche Nutzung festgestellt, ist dies unverzüglich an [canvas@hs-aalen.de](mailto:canvas@hs-aalen.de) zu melden.
- Für die Registrierung zu Prüfungen sind nur Accounts zugelassen, welche die offiziell zugewiesene Hochschulmailadressen nutzen. Ist eine andere Mail hinterlegt, da kein Hochschulkonto existiert, ist die Nutzung vorher mit dem Canvas-Kernteam zu klären.
- Aufsichten dürfen nur mit einer Hochschulmailadresse eingeladen werden.
- Die Aufnahmen werden zwei Wochen nach Ende des Prüfungszeitraums gelöscht. Wird ein Täuschungsversuch festgestellt, kann die Löschung einzelner Aufnahmen als Nachweis bis vier Wochen nach dem Prüfungszeitraum verschoben werden, maximal allerdings bis zur Entscheidungsfindung über den Vorfall. Zur Verlängerung der Löschfrist sind folgende Informationen notwendig:
  - Exam-ID / Link zur Prüfung
  - Student-ID der Person, bei welcher ein Verdacht vorliegtDiese Informationen sind bis spätestens ein Tag vor zwei Wochen nach dem Prüfungszeitraum an [canvas@hs-aalen.de](mailto:canvas@hs-aalen.de) zu melden.

### Kontakt

Bei Fragen zur Nutzung des Systems steht Ihnen das Canvas-Kernteam ([canvas@hs-aalen.de](mailto:canvas@hs-aalen.de)) zur Verfügung.

## **Anlage 7: Infoschreiben Studierende**



## Hinweise zum Datenschutz – Einsatz von „DigiExam“ an der Hochschule Aalen

Angesichts der aktuellen SARS-CoV-2-Krisensituation und den damit verbundenen Einschränkungen stehen alle Bildungseinrichtungen vor der großen Herausforderung, Prüfungen durchzuführen. In dieser besonderen Lage bietet eine Proctoring Software eine Option, die es den Studierenden erlaubt, Ihre Prüfungsleistungen von Zuhause aus zu erbringen und gleichzeitig hinreichend Gewähr für eine täuschungsfreie Leistung bietet. Zur Bewältigung der aktuellen Krise muss trotz zum Teil bestehender datenschutzrechtlicher Bedenken, ergänzend auf Proctoring Software zurückgegriffen werden.

Hochschulen werden besonders gefordert, weil sich die Lehrangebote oft an große Teilnehmergruppen richten. Die bestehenden bzw. lokal gehosteten Systeme können zwar für wenige kleine Veranstaltungen verwendet werden, jedoch führt die erforderliche große Zahl an gleichzeitigen digitalen Prüfungsveranstaltungen mit großen Teilnehmergruppen, diese Systeme an die Leistungsgrenzen. So kann die Hochschule, insbesondere im Bereich der Lehre, ihrer gesetzlichen Aufgabenerfüllung derzeit nur nachkommen, wenn ergänzend Angebote externer Anbieter eingesetzt werden.

Insofern wurde für die Durchführung von Online-E-Klausuren sowie Testaten ein Kontingent an Lizenzen für die Proctoring-Lösung der Firma DigiExam beschafft. Die Entscheidung für DigiExam ist gefallen, weil dieser Anbieter seinen Sitz in der Europäischen Union hat und somit den in der Europäischen Union geltenden Datenschutzstandards unterliegt. Ferner haben technische Tests eine hohe Zuverlässigkeit gezeigt. Der Dienst wird an der Hochschule Aalen in Situationen eingesetzt, in denen Präsenzveranstaltungen nicht möglich sind und nicht auf hochschuleigene Systeme zurückgegriffen werden kann. Lehrende und Studierende sind zur Nutzung von DigiExam mit Proctoring-Funktion nicht verpflichtet. Die Proctoring-Funktion wird nur beim Schreiben von Online-E-Klausuren zu Hause aktiviert. Alternativ wird eine Möglichkeit angeboten, die Klausur am PC in den Räumlichkeiten der Hochschule mit oder ohne Proctoring zu schreiben.

## Inhalt

1. Informationsschreiben nach Art. 13 DSGVO .....	2
2. Umfang der Verarbeitung.....	2
3. Zwecke und Rechtsgrundlage der Verarbeitung.....	4
4. Empfänger der Daten.....	4
5. Speicherdauer.....	5
6. Rechte der betroffenen Personen.....	5

## 1. Informationsschreiben nach Art. 13 DSGVO

Die Hochschule Aalen verarbeitet personenbezogene Daten im Zusammenhang mit der Durchführung von Online-Prüfungen unter Einsatz des Dienstleisters „DigiExam“.

Mit diesem Datenschutzhinweis möchte die Hochschule Aalen gemäß Art. 13 DSGVO über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen von Online-E-Klausuren und Testaten informieren.

### Name und Kontaktdaten des für die Datenverarbeitung Verantwortlichen

Hochschule Aalen  
Adresse: Beethovenstraße 1, 73430 Aalen  
Telefon: 07361 576-0  
E-Mail: [info@hs-aalen.de](mailto:info@hs-aalen.de)

### Kontaktinformationen der/des Datenschutzbeauftragten

Hochschule Aalen  
Adresse: Beethovenstraße 1, 73430 Aalen  
E-Mail: [datenschutz@hs-aalen.de](mailto:datenschutz@hs-aalen.de)

## 2. Umfang der Verarbeitung

### Folgende personenbezogene Daten sind Gegenstand der Verarbeitung:

Angaben zum Benutzer: Die Anmeldung zur jeweiligen Prüfung in DigiExam erfolgt unter Anwendung von Ihren Canvas-Zugangsdaten. Die dort hinterlegten Daten werden zwecks Anmeldung und Authentifizierung verarbeitet. Dazu gehören Ihr

Vorname, Nachname, Student-Code (i.d.R. E-Mailadresse), E-Mail-Adresse; alternativ kann die Anmeldung über eine Exam-ID direkt in der Anwendung DigiExam erfolgen. Hierbei müssen von Ihnen folgende Daten angegeben werden: Ihr Vorname, Nachname, Student-Code (i.d.R. E-Mailadresse), E-Mail-Adresse;

**Metadaten:** Teilnehmer-IP-Adressen, Geräte-Hardware-Informationen; Video-, Audio- und Bildschirmdaten:

- Während der Dauer der Prüfung (von Starten der Prüfung im DigiExam Client bis zur Abgabe der Prüfungsleistung) werden die Daten vom Mikrofon sowie von der Videokamera des Endgeräts, sowie eine Aufnahme des Bildschirms verarbeitet, sofern die Proctoring Funktion aktiviert ist. In diesem Zeitraum wird ferner zwecks Verhinderung von Täuschungsversuchen eine Gesichtserkennung unter Verarbeitung Ihrer biometrischen Daten durchgeführt.
- Eine Bildaufnahme von Ihrem Gesicht wird im Speicherbereich von DigiExam auf einer Google Cloud Infrastruktur in Belgien in verschlüsselter Zustand abgelegt. Ihr Bild wird einer Sitzung zugeordnet. Die Sitzung selbst wird einem Studierenden und der jeweiligen Prüfung zugeordnet.
- Zudem werden biometrische Gesichtsmerkmale, im Sinne des Art. 9 Abs (1) DSGVO, aus diesem Bild extrahiert, die zur Feststellung dienen, ob sich über den Verlauf der Prüfung immer dieselbe Person vor der Kamera befindet. Diese Daten werden in einer Datenbank gespeichert, welche von einem Auftragsverarbeiter von DigiExam in Europa betrieben wird. Der Eintrag in der Datenbank wird der Sitzung zugeordnet.
- Die Audio-, Video-, und Bildschirmdaten werden ab Starten der Prüfung im DigiExam Client bis zur Abgabe der Prüfungsleistung zwecks einer täuschungsfreien Prüfungsdurchführung aufgenommen. Die Videodaten bestehen aus Videosequenzen, die lokal aufgenommen und während der Sitzung ununterbrochen an DigiExam geschickt werden. Diese Daten werden auf den Data-Storage-Servers von Google Cloud in Belgien verschlüsselt gespeichert. Die Entschlüsselung kann nur durch einen autorisierten Zugriff durch Entwickler oder der Proctoring Software erfolgen. Die Videodaten werden der Sitzung zugeordnet.
- Die Audiodaten werden lediglich als Anwesenheit von Audiosignalen von dem Programm verarbeitet.
- Der für die jeweilige Aufsichtsperson während der Online-E-Klausur sichtbare Videostream selbst wird weder aufgenommen noch gespeichert.
- Es werden allgemeine Informationen zur Hardware (Bildschirmauflösung, Betriebssystem und IP-Adresse, sowie ein Client-Hash gespeichert, um Fehler nachvollziehen und beseitigen zu können.

## **Textdaten:**

Sie haben die Möglichkeit, während der Online-E-Klausur die Aufsichtsperson per Chat zu kontaktieren. Bei Kontaktaufnahme zur Aufsichtsperson werden die Uhrzeit sowie der Chat-Verlauf gespeichert.

### **3. Zwecke und Rechtsgrundlage der Verarbeitung**

Ihre personenbezogenen Daten werden von der Hochschule Aalen zum Zweck der täuschungsfreien Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation verarbeitet.

Die Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten ist Ihre Einwilligung gemäß Art. 9 Abs. 2 lit. a) DSGVO, die Sie vor der Prüfungsteilnahme beim zuständigen Prüfungsamt abgegeben haben. Im Übrigen ist die Rechtsgrundlage Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO.

Neben der Möglichkeit eine Online-E-Klausur mit Proctoring unter Anwendung von DigiExam zu schreiben, besteht weiterhin die Möglichkeit an einer Präsenzklausur teilzunehmen. Entscheiden Sie sich für die Präsenzklausur, so bitten wir um eine verbindliche Mitteilung spätestens zwei Wochen vor dem jeweiligen Klausurtermin, damit wir die notwendigen organisatorischen Vorkehrungen treffen können.

Ihre Einwilligung können Sie jederzeit gegenüber dem Prüfungsamt oder gegenüber der, während der Online-E-Klausur vertretenden, Aufsichtsperson widerrufen. Aus dem Widerruf oder aus der Nicht-Erteilung der Einwilligung entstehen Ihnen keinerlei Nachteile.

Soweit personenbezogene Daten von Beschäftigten der Hochschule Aalen verarbeitet werden, ist Art. 6 Absatz 1 UA 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. Landesbeamtengesetz BW (LBG) die Rechtsgrundlage der Datenverarbeitung.

### **4. Empfänger der Daten**

Personenbezogene Daten, die im Zusammenhang mit der Teilnahme an Online-E-Klausuren verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht gerade zur Weitergabe bestimmt sind. Der Anbieter von „DigiExam“ erhält notwendigerweise Kenntnis von den o. g. Daten, soweit dies im Rahmen des Auftragsverarbeitungsvertrages mit „DigiExam“ vorgesehen ist. „DigiExam“ ist ein Service der DigiExam Solutions Sweden AB., die ihren Sitz in Schweden hat.

## 5. Speicherdauer

Wird das Vorliegen einer täuschungsfreien Prüfungsleistung durch Bewertung festgestellt, so werden die personenbezogenen Video-, Audio- sowie Bildschirmdaten unverzüglich gelöscht. Bestehen durch Tatsachen begründete Zweifel, ob eine täuschungsfreie Prüfungsleistung vorliegt, so werden Ihre personenbezogenen Daten bis zur Feststellung, ob eine Täuschung vorliegt, gespeichert. Wird der Verdacht ausgeräumt, erfolgt die Löschung unverzüglich nach der Bewertung. Bei einer nachgewiesenen Täuschung werden die personenbezogenen Daten bis zum Ende des Folgejahres nach Abschluss des Prüfungsverfahrens gespeichert.

Alle Prüfungsergebnisse werden bis zum Ende des Folgejahres nach Abschluss des Prüfungsverfahrens gespeichert. Das Gleiche gilt für den Fall, dass ein gegen die Prüfungsbewertung gerichtetes Widerspruchs- bzw. Klageverfahren noch nicht rechtskräftig abgeschlossen ist.

## 6. Rechte der betroffenen Personen

Nach der DSGVO stehen Ihnen unter den im Gesetz genannten Voraussetzungen folgende Rechte zu:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO),
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO),
- Widerspruchsrecht (Art. 21 DSGVO).

Zudem haben Sie das Recht der Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO). Aufsichtsbehörde im Sinne des Art. 51 Abs. 1 DSGVO über die Hochschule Aalen ist gemäß § 25 Abs. 1 LDSG der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de).

**Anlage 8: Einwilligungserklärung Studierende**

# 1. Unverbindliche Anmeldung zur Teilnahme an Online-Prüfungen

Unabhängig davon, ob Prüfungen in Präsenz oder als Onlineprüfung abgehalten werden, melde ich

Name, Vorname: \_\_\_\_\_

Matrikelnummer: \_\_\_\_\_

Studiengang: \_\_\_\_\_

mich hiermit unverbindlich zu der Variante Online-E-Prüfung für die von mir angemeldeten Prüfungen im Wintersemester 2020/21 bei der Hochschule Aalen an.

Prüfungs-Nr.	Modulbezeichnung	Prüfungsform	Prüfer

(bitte entsprechend angemeldete Prüfungen eintragen)

Mir ist bekannt, dass eine verbindliche Prüfungsanmeldung erst mit der Anmeldung im OnlinePrüfungsraum oder durch persönliches Erscheinen am Tag der Prüfung erfolgt. Für den Fall, dass ich mich am Prüfungstag nicht im Online-Prüfungsraum anmelde, erwachsen mir keine Nachteile aus der Nichtteilnahme. Der Abbruch einer bereits angetretenen Prüfung wird als Fehlversuch gewertet.

Ich willige ein, dass ich während der Online-Prüfung zur Sicherstellung eines ordnungsgemäßen Prüfungsablaufs, insbesondere zur Vermeidung von Täuschung oder Benutzung nicht zugelassener Hilfsmittel, durch die Hochschule Aalen über DigiExam in meiner Wohnung visuell und akustisch beaufsichtigt werde.

---

(Ort, Datum, Unterschrift)

Bitte füllen Sie vorstehende Daten aus. Wir bitten um Rücksendung (postalisch oder per Mail „pruefungsamt@hs-aalen.de“) an das Zentrale Prüfungsamt der Hochschule Aalen bis spätestens 13. Januar 2021. Teilnehmer der externen Studienangebote des Graduate Campus und der Graduate School Ostwürttemberg wenden sich bitte an externe-stg@hs-aalen.de. Frist zur Einreichung ist der jeweilige Anmeldeschluss.

## 2.DATENSCHUTZRECHTLICHE EINWILLIGUNGS-ERKLÄRUNG

Die Hochschule Aalen bietet in der SARS-CoV-2-Krisensituation neben der regulären Durchführung einer Präsenzprüfung am jeweiligen Prüfungstermin oder zu einem späteren Zeitpunkt an, die Prüfungen als digitale Online-Prüfungen (Online-E-Klausur) unter Anwendung von DigiExam durchzuführen. Gemäß Art. 6 UAbs. 1 Buchstabe e) DS-GVO ist es der Hochschule gestattet, personenbezogene Daten der Studierenden zu verarbeiten, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt. Soweit auf freiwilliger Basis weitere Daten zwecks Reduktion der Täuschungsmöglichkeiten erhoben werden, wird eine Einwilligung benötigt.

Hiermit willige ich

Name, Vorname: \_\_\_\_\_

Matrikelnummer: \_\_\_\_\_

Studiengang: \_\_\_\_\_

in das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Auslesen, das Abfragen, die Verwendung, den Abgleich oder die Verknüpfung, das Löschen oder die Vernichtung **meiner folgenden personenbezogenen Daten**

Vorname, Nachname, Matrikelnummer, E-Mail-Adresse, Teilnehmer-IP-Adressen,

GeräteHardware-Informationen, Bildschirmdaten, Textdaten des Chat-Verlaufs,

Prüfungsleistung **sowie folgender besonderer Kategorien personenbezogener Daten**

während der Prüfung aufgenommene Video- und Audiodaten, Gesichtsbild, biometrische Daten des Gesichtsbildes, Videostream durch die Hochschule Aalen ein.

Die Datenverarbeitung erfolgt ausschließlich zu folgenden Zwecken:

- Durchführung der Remote-Aufsicht bei der digitalen Online-E-Klausur

Prüfungs-Nr.	Modulbezeichnung	Prüfer	Einwilligung Ja
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>

(bitte entsprechende Prüfungen eintragen und ggf. Einwilligung erteilen)

- Feststellung der Täuschungsfreiheit der Prüfungsleistung zwecks Bewertung der Prüfungsleistung;



- Auswertung der Daten bei begründetem Verdacht einer Täuschung;
- Feststellung der Täuschung;
- Beweisführung in einem eventuellen Widerspruchs- bzw. Klageverfahren;

Die Einwilligung erfolgt auf freiwilliger Basis. Mir ist bekannt, dass die Einwilligung jederzeit und ohne Angabe von Gründen widerrufen werden kann. Im Fall des Widerrufs dürfen die bereits erhobenen Daten ab Zugang der Widerrufserklärung nicht mehr für die oben genannten Zwecke verwendet werden.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung nicht berührt. Mir ist klar, dass für mich aus Verweigerung der Einwilligung oder ihrem Widerruf keine Nachteile entstehen. Meine Widerrufserklärung kann ich schriftlich oder in Textform an die Hochschule Aalen richten.

Nach der DSGVO stehen Ihnen unter den im Gesetz genannten Voraussetzungen folgende Rechte zu:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO),
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO),

Zudem haben Sie das Recht der Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO). Aufsichtsbehörde im Sinne des Art. 51 Abs. 1 DSGVO über die Hochschule Aalen ist gemäß § 25 Abs. 1 LDSG der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de).

---

(Ort, Datum, Unterschrift)

Bitte füllen Sie vorstehende Daten aus. Wir bitten um Rücksendung (postalisch oder per Mail „[pruefungsamt@hs-aalen.de](mailto:pruefungsamt@hs-aalen.de)) an das Zentrale Prüfungsamt der Hochschule Aalen bis spätestens 13. Januar 2021. Teilnehmer der externen Studienangebote des Graduate Campus und der Graduate School Ostwürttemberg wenden sich bitte an [externestg@hs-aalen.de](mailto:externestg@hs-aalen.de). Frist zur Einreichung ist der jeweilige Anmeldeschluss.

### 3. Bestätigung der Teilnahme an einer oder mehreren Online-Testklausur/en

Hiermit bestätige ich, dass ich als Voraussetzung für die Teilnahme an Online-E-Klausuren an mindestens einer oder mehreren Online-Testklausuren entweder im Rahmen des Prüfungszeitraums des Sommersemesters 2020 oder Wintersemester 2020/21 teilgenommen habe bzw. bis zum Prüfungszeitraum des Wintersemesters 2020/21 noch teilnehmen werde.

---

(Ort, Datum, Unterschrift)

Bitte füllen Sie vorstehende Daten aus. Wir bitten um Rücksendung (postalisch oder per Mail „[pruefungsamt@hs-aalen.de](mailto:pruefungsamt@hs-aalen.de)) an das Zentrale Prüfungsamt der Hochschule Aalen bis spätestens 13. Januar 2021. Teilnehmer der externen Studienangebote des Graduate Campus und der Graduate School Ostwürttemberg wenden sich bitte an [externestg@hs-aalen.de](mailto:externestg@hs-aalen.de). Frist zur Einreichung ist der jeweilige Anmeldeschluss.

## 4. Eigenständigkeitserklärung

Hiermit erkläre ich, dass alle im Prüfungszeitraum des Wintersemesters 2020/21 von mir abgelegten Online-E-Klausuren auch von mir selbstständig verfasst und keine anderen als die angegebenen erlaubten Quellen und Hilfsmittel benutzt wurden.

---

(Ort, Datum, Unterschrift)

Bitte füllen Sie vorstehende Daten aus. Wir bitten um Rücksendung (postalisch oder per Mail „pruefungsamt@hs-aalen.de“) an das Zentrale Prüfungsamt der Hochschule Aalen bis spätestens 13. Januar 2021. Teilnehmer der externen Studienangebote des Graduate Campus und der Graduate School Ostwürttemberg wenden sich bitte an externe-stg@hs-aalen.de. Frist zur Einreichung ist der jeweilige Anmeldeschluss.

## 5. Einwilligungserklärung zur Datenerhebung im Rahmen der Nutzung der Hotline

Ich bin damit einverstanden, dass sofern ich während einer Online-E-Prüfung die Hotline zur Klärung von Problemen kontaktieren werde/muss, nachstehende Daten dokumentiert und in meiner Studierendakte abgelegt werden. Ggf können diese Daten zum Zwecke der Klärung von prüfungsrechtlichen Fragen im Rahmen eines Widerspruch- bzw. Klageverfahren an den zuständigen Prüfungsausschuss meines Studiengangs, das zentrale Prüfungsamt der Hochschule Aalen oder an weitere beteiligte Stellen weitergeleitet werden

Erhobene Daten:

- Matrikelnummer des Prüflings
- Name, Vorname des Prüflings
- Ort der Prüfungsdurchführung (zu Hause oder an der Hochschule, etc.)
- Prüfungsart
- Name des Prüfers / ggf. Zweitprüfers
- Uhrzeit - Auftreten des Problems
- Uhrzeit des Anrufs
- Problem des Prüflings

---

(Ort, Datum, Unterschrift)

Bitte füllen Sie vorstehende Daten aus. Wir bitten um Rücksendung (postalisch oder per Mail „pruefungsamt@hs-aalen.de“) an das Zentrale Prüfungsamt der Hochschule Aalen bis spätestens 13. Januar 2021. Teilnehmer der externen Studienangebote des Graduate Campus und der Graduate School Ostwürttemberg wenden sich bitte an externe-stg@hs-aalen.de. Frist zur Einreichung ist der jeweilige Anmeldeschluss.

Bitte beachten Sie, dass ohne die umseitig/ bzw. oben genannte Vorläufige Anmeldung zur

Online-E-Klausur, datenschutzrechtliche Einwilligungserklärung, der Bestätigung der Teilnahme an einer oder mehreren Online-Testklausuren, der Eigenständigkeitserklärung, Einverständniserklärung zur Datenerhebung und der Rücksendung dieses Formulars bis 13. Januar 2021 eine Teilnahme an einer Online-E-Klausur nicht möglich ist. Frist für die

externen Studienangebote ist auch hier der jeweilige Anmeldeschluss zur Prüfung. Die Prüfung/en wird/werden ggf. seitens des Zentralen Prüfungsamtes abgemeldet.