Anlage 13: Information Security Policy (DigiExam)

Information Security Policy

10.5 Public APIs

Document owner: [redacted]
Minimum review interval: Biennial
Version: 1.1

Versions

Version	Date	Author	Description
1.2	2021-03-09	[redacted]	[redacted]
1.1	2020-11-03	[redacted]	[redacted]
1.0	2018-04-09	[redacted]	[redacted]

Introduction

DigiExam will protect all information that our businesses handles. This is a necessity in order to achieve our different business goals and for our clients, partners, owners and employees should have confidence and trust in DigiExam.

DigiExam is working actively with information security to sustain that all our data is classified and set to the right level of confidentiality, integrity and availability. DigiExam apply a common and structured way of working with information security based on international standard for ISMS (Information Security Management System).

With the support of ISMS, DigiExam create the right level of information security on a daily basis. Information security work is a long term goal and a continuous work; covering all aspects of our business and all of the information assets we own or and manage. Staff and contractors receive continuous training to understand how information security works.

DigiExam, and everyone within, is responsible for the safeguarding of our information. Whomever discovers deficiencies in information security shall notify their manager or the security manager. Events that present a risk for our information assets must also be reported instantly. Responsibility for the information security is operational and the line manager's duty.

Definitions:

- Information assets are anything that contains information or carries information.
- Information security is security regarding information assets related to the ability to maintain the desired confidentiality, integrity and availability.

The ISMS helps us to establish, implement, operate, monitor, review, maintain and improve the desired level of information security for DigiExam.

Security Incident Response Plan

[redacted]

Communication to be done

[redacted]

Information to be included

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

General Security Compliance

[redacted]

Classification of data processed in the service

[redacted]

Historical incidents of data breach

[redacted]

Network and Infrastructure

[redacted]

Data center location: [redacted]

Compliance

T[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Encryption of data

[redacted]

Security audits

Internal security audits

[redacted]

Third-party security audits

[redacted]

Automated vulnerability scanning

[redacted]

Client initiated security audits

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Operations and continuity

Monitoring

[redacted]

Uptime monitoring

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

Detailed service monitoring

[redacted]

Redundancy and scaling

[redacted]

Load testing

[redacted]

Student client redundancy

[redacted]

Denial-of-Service protection

[redacted]

Backups

Customer data

[redacted]

Service source code

[redacted]

Staging environments

[redacted]

- [redacted]
- [redacted]

Continuous integration

[redacted]

Automatic code quality checks

[redacted]

- [redacted]
- [redacted]
- [redacted]

Maintenance periods

[redacted]

Outage escalation plan

[redacted]

Platform compatibility strategy

[redacted]

Other routines

[redacted]

Human Resources

Background checks

[redacted]

Employee compliance training

[redacted]

Non-disclosure agreement

[redacted]

Employment termination

[redacted]

Security Controls

Remote access

[redacted]

Workstation security

[redacted]

Storage device disposal

[redacted]

Configuration management and patching

[redacted]

Authentication of callers

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

Multi-tenancy security controls

[redacted]

Access and audit logs

Physical access

[redacted]

Audit logs

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Customer data access - audit logs

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

Monitoring of audit and access logs

[redacted]

Event logs

[redacted]

- [redacted]
- [redacted]
- [redacted]

- [redacted]
- [redacted]

HTTP logs

[redacted]

Interoperability and portability

LTI 1.0 and 1.1

[redacted]

- [redacted]
- [redacted]
- [redacted]

QTI 1.2 data import

[redacted]

SAML 2.0 (Single-sign-on)

[redacted]

Data export

[redacted]

- [redacted]
- [redacted]

Public APIs

[redacted]

Anlage 14: Privacy Policy (DigiExam)

DigiExam

PRIVACY POLICY

Last updated: 2020-08-25

DigiExam Solutions Sweden AB
Smidesvägen 10
171 41 Solna
Sweden

DigiExam

We at DigiExam Solutions Sweden AB ("DigiExam," "we," "us," "our") know that our users ("you," "your") care about how your personal information ("Personal Data") is used and shared, and we take your privacy seriously. We will be transparent with you about the type of Personal Data we collect and provide clear information about how we use that Personal Data. We have taken proper measures to ensure that we follow all applicable data protection laws and regulations and we will co-operate with the authorities when needed. In the absence of data protection legislation, we will act in accordance with generally accepted principles governing data protection.

This policy ("Privacy Policy") describes: (i) the types of Personal Data we collect when you use our service or website; (ii) why and how we use that Personal Data and what security measures we take in order to protect that Personal Data; (iii) how long we retain it; and (iv) with whom we share it. It also explains what your rights and options are as they pertain to privacy. By visiting this website or using our service, you acknowledge our collection and use of your Personal Data as described in this Privacy Policy.

We strongly suggest that you read this Privacy Policy, and contact us if you have any questions.

IMPORTANT NOTICE FOR STUDENTS AND TEACHERS: This Privacy Policy does not govern the collection, use, or disclosure of Personal Data through the use of the service by the educational institution which has given you access to the service, . Please contact this organization to better understand its privacy practices as data controller. DigiExam will retain Personal Data we process on behalf of organizations for as long as needed to provide services and as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements as data processor

What Does This Privacy Policy Cover

This Privacy Policy covers our treatment and processing of Personal Data (any directly or indirectly personally identifiable information) that DigiExam gathers when you are accessing or using our website or services. *Processing* refers to any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data We Collect and Why

Data You Provide to Us

We receive and store any Personal Data you actively provide to us. The only Personal Data required from you in order to register or log onto our service is your full name, e-mail address and student code. The student codes are collected and used by schools in order to identify their students. The type of student code used varies depending on the school's policy and can consist of an e-mail address, personal identity number or the first letters in the student's first and last name.

In the future, we may ask for additional Personal Data to enhance your profile, such as education, interests, and communication preferences. Any such data you elect to add to your account in this regard is voluntary.

You can choose not to provide us with certain Personal Data but then you may not be able to register with us or to take advantage of some of our features or services. We may anonymize your Personal Data so that you cannot be individually identified either directly or indirectly.

DigiExam

Data Collected Automatically

Whenever you interact with our service, we automatically receive and record data on your computer properties ("Log data"). For example, Log data may include data such as your computer's IP address, type and version of operating system, the screen resolution of your computer etc. Client hash is also collected by us in order to identify a student's computer when there has been a computer error.

Whenever you interact with our website, certain information is also provided to us from your browser via e.g. cookies. Cookies are identifiers, files or pieces of information, which we transfer to the computer or mobile device you are using that allow us to recognize the browser or mobile device and tell us how and when pages in our website are visited by you. Cookies may provide information on, inter alia, browser type, how you navigate on our website and other statistics. Some of this information may constitute Personal Data to the extent it can be traced back to an individual. We use this information for our legitimate interest to monitor and analyze the use of our website in order to increase our website's functionality and user-friendliness to better tailor it to your needs. Various browsers may offer their own management tools for removing cookies. Most web browsers are set to accept cookies by default. You may be able to change the preferences on your browser or mobile device to delete or to prevent or limit your computer or device's acceptance of cookies, but that may affect the functionality of our website.

Please refer to our cookie policy for details regarding the types of cookies used.

Our website includes social media features. These features may collect your IP address, which page you are visiting on our website, and may set a cookie to enable the feature to function properly. Social Media features and widgets are either hosted by a third party or hosted directly on our website. Your interactions with these features are governed by the privacy statement of the company providing it.

We use analytics services to help analyze how users use our website. These services use cookies and scripts to collect and store data such as user interaction, errors users encounter, device identifiers, how often users visit the site, what pages they visit, and what other sites they used prior to coming to the site. You may opt out of tracking of certain information collected by Google Analytics on the website by clicking here.

Please see the following links for more information about GoogleAnalytics: http://www.google.com/privacy_ads.html, http://www.google.com/privacy.html, and http://www.google.com/analytics/tos.html.

For What Purpose We Use Your Personal Data and Based on What Legal Grounds

We use the data we receive from you in order to fulfill our agreements with our customers as a data processor and for our legitimate business interests in order to operate, administrate/maintain and improve our website and our service including responding to requests that you make, or otherwise to aid us in serving you better or in order to comply with the law as set out in section D below. In particular, we use your Personal Data in the following ways: to create and maintain your account; to identify you as a user in our system; to operate, maintain, and improve our website and our services and to personalize and improve your experience; to send you administrative emails and to respond to your comments or inquiries. We have a legitimate interest to send you surveys, promotional communication and information about product and service updates with your permission when logging onto our site; to protect, investigate, and deter against fraudulent, unauthorized, or illegal activity; and to contact you as a part of secondary fraud protection or to solicit your feedback with your permission.

We may also use general data that we collect from you which does not contain Personal Data for our own internal purposes (i.e., to monitor overall usage trends, metrics, page views, etc.).

Communication

We have a legitimate interest to communicate to our users and may contact you, by email or other means. If you wish to subscribe to our newsletter(s), we will use your name and email address to send the newsletter to you. Out of respect for your privacy, you may choose to stop receiving our newsletter or marketing emails by following the unsubscribe instructions included in these emails. You can also always contact us at privacy@digiexam.com if you do not wish to receive any email or contact from us. Please note however, that if you do not want to receive legal notices from us, those legal notices will still govern your use of the website, and you are responsible for reviewing such legal notices for changes. Such legal notices and the complete set of updated terms are to be found on our website.

Testimonials

We may post user testimonials/comments/reviews on our website which may contain Personal Data. We do obtain the user's consent via email or another suitable channel prior to posting the testimonial including Personal Data. Such consent may be withdrawn at any time. To request removal of your Personal Data from Testimonials or comments please contact us at privacy@digiexam.com

Where We Store Your Personal Data

Your Personal Data is stored on a cloud platform provided by Google. If you are located outside the European Union, the Personal Data that we collect from you may be transferred to, and stored and processed at, a destination in the European Union. We will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this Privacy Policy. We use subprocessors who receive and process certain Personal Data on our behalf. Please click here for a complete list of all our subprocessors and where they store their data.

Disclosure of Your Personal Data

We will not sell or lease any of your Personal Data in personally identifiable form to anyone. We share such Personal Data in personally identifiable form with third parties as described below.

A. Trusted Third Parties: We employ other companies and people to perform tasks on our behalf and need to share your Personal Data with them to provide the services to you. Unless we tell you differently, such third parties do not have any right to use the Personal Data we share with them beyond what is necessary to assist us. This includes third party companies and individuals employed by us to facilitate and improve our services, including the provision of maintenance services, database management, Web analytics and general improvement of the services.

B. Educational institution or other course provider: We will share your Personal Data with the educational institution or organization which is linked to your use of the services. For example, this would apply:

- If teachers, administrators and account managers use the platform, for example when teachers use the service in order to prepare and administrate exams ; or

- If you as a student are conducting a test, whereby we will share your data including test results with the educational institution providing the test, including teachers.

C. Business Transfers: *We may choose to buy or sell assets. In these types of transactions,* Customer data is typically one of the business assets that is transferred. Also, if we (or substantially all of our assets) are acquired, or if we go out of business, enter into bankruptcy, or go through some other change of control, Personal Data would be one of the assets transferred to, or acquired by, a third party. You will be notified via email of any change in ownership or uses of your Personal Data, including a reference to a prominent notice and information on our website as well as a notice when logging onto our service. You will also be informed of any choices you may have regarding your Personal Data.

D. Protection of DigiExam and Others: We reserve the right to access, read, preserve, and disclose any data that we reasonably believe is necessary to comply with law or a court order; enforce or apply our conditions of use and other agreements; or protect the rights, property, or safety of DigiExam, our employees, our users, or others. This includes exchanging data with other companies and organizations for fraud protection and credit risk reduction. We also may be required to disclose an individual's Personal Data in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

Except as set forth above, you will be notified when your Personal Data may be shared with third parties, and you will be able to prevent the sharing of such Personal Data.

General Practices Related to Data Security

We take the security of your Personal Data seriously and use appropriate measures to protect it against unauthorized or unlawful processing and against accidental loss, destruction or damage. Our security measures are constantly being revised in accordance with technological developments. Which actions that are necessary will depend on the type of Personal Data being processed and the specific risks associated with that processing.

You must prevent unauthorized access to your account and Personal Data by protecting your credentials appropriately and limiting access to your computer or device and browser by signing off after you have finished accessing your account.

DigiExam is committed to maintaining the security and confidentiality of a user's Personal Data. To that end, DigiExam has taken the following actions: (a) limiting employee access to Personal Data pertaining to students based on roles and responsibilities; (b) conducting background checks on employees who have access to student data; (c) conducting privacy training for employees with access to students' Personal Data; (d) protecting Personal Data with technical, contractual, administrative, and physical security safeguards in order to protect it from unauthorized access, release or use.

When you enter your Personal Data on our site we encrypt the transmission of that Personal Data using transport layer security (TLS).

Whenever your Personal Data is used for purposes such as statistics or general user activity monitoring we make sure to anonymize the data where appropriate.

Our website or tests provided in the service may contain links to other sites. We are not responsible for the privacy policies and/or practices on other sites. When following a link to another site you must read that site's Privacy Policy. If you share your computer or use a computer that is accessed by the general public, remember to sign off and close your browser window when you have finished your session.

Data Breach

If DigiExam is notified about a security breach of a system by an unauthorized party or that any user's Personal Data was used for an unauthorized purpose, we will comply with applicable data protection legislation regarding data breaches and use appropriate measures to mitigate the breach.

Your Control Over Personal Data

As a data subject you have many rights regarding your Personal Data which is collected and stored. In summary, these include:

(i) the right to transparency and access with respect to the Personal Data that is stored and processed,

(ii) the right to corrections of any mistakes in the Personal Data and erasure in certain situations,

(iii) the right to restriction of processing in certain circumstances,

(IV) the right to object at any time to processing of Personal Data concerning you when such processing is based on our legitimate interest, for direct marketing and in certain other situations

(V) the right to lodge a complaint with a data protection supervisory authority,

(VI) the right to data portability, i.e. to receive Personal Data collected about you in a structured, *commonly used and machine-readable format, and*

(VII) the right to claim compensation for damages caused by our breach of any data protection legislation.

You may access, and, in some cases, edit, update or delete Personal Data you have provided to us. You have the right to decline to share certain elements of Personal Data that we ask you to provide, but keep in mind that the Personal Data may be needed to use our services. We may use any aggregated data derived from or incorporating your Personal Data after you update or delete it, but not in a manner that would identify you personally.

The Personal Data you can view, update, and delete may change as the website changes. If you have any questions about viewing or updating Personal Data we have on file about you, please contact us at privacy@digiexam.com. We will respond to your request to access within 30 days.

How Long We Keep Personal Data

Personal Data will never be stored longer than necessary in view of the above-mentioned purposes. The criteria for determining the retention period are based on our agreement with your educational institution, the legal obligations we have to adhere to, and our legitimate interest to communicate with you in order to manage the service and any user problems that can occur, as well as marketing purposes. The same Personal Data can be stored in different locations for different purposes. Your Personal Data is only accessible by authorized personnel.

In general, we will retain your Personal Data for as long as your account is active or as needed to provide you services. You may request deletion of your account by contacting us at privacy@digiexam.com. All of your Personal Data will be deleted from our database or de-identified when the account is closed.

We will store the Personal Data per the user's license requirement or delete the account upon user request. For database backups, we do a daily backup which is stored up to 90 days. Log data is stored up to 180 days.

Our current data retention policy is to keep each student's data within the active contract period or a minimum duration required for licensing compliance per request from the Customer within the active contract period. We may also choose to anonymize certain parts of the Personal Data you provide to us so that it can no longer be attributed to you if we would like to retain it for longer periods of time.

Changes to This Privacy Policy

DigiExam reserves the right, at its sole discretion, to modify, add or remove portions of this Privacy Policy from time to time. We will note any such changes by updating the publication date of this Privacy Policy and inform our users of this when logging onto our platform including a link to the downloadable Privacy Policy on our website. It is each user's responsibility to review the Privacy Policy when it is changed.

If we make significant changes impacting the collection, use, disclosure or retention of Personal Data, we will also provide an email notice to you thirty (30) days in advance of implementing those changes.

Questions or Concerns

If you have any questions or concerns regarding our privacy policies, please send us a detailed message privacy@digiexam.com. We will make every effort to resolve your concerns.

Contact Information

DigiExam Solutions Sweden AB
Attn: Data Protection Officier
Address: [redacted]
Tel: [redacted]
Email: privacy@digiexam.com

Verzeichnis von Verarbeitungstätigkeiten

des Verantwortlichen gemäß Art. 30 Abs. 1 DSGVO

ALLGEMEINER TEIL

Angaben zum Verantwortlichen		**Angaben zur Person des Datenschutzverantwortlichen**
Name	Hochschule Aalen	
Straße	Beethovenstraße 1	Beethovenstraße 1
PLZ, Ort	73430 Aalen	73430 Aalen
Land	Deutschland	Deutschland
Telefon	07361 576-0	07361 576-xxxx
E-Mail-Adresse	info@hs-aalen.de	datenschutz@hs-aalen.de

Hinweis:
Dies ist ein statisches Vorblatt, Änderungen werden hier nur von zentraler Stelle vorgenommen!

Verzeichnis von Verarbeitungstätigkeiten
des Verantwortlichen gemäß Art. 30 Abs. 1 DSGVO

BESONDERER TEIL

Beschreibung der Verarbeitungstätigkeit

Beschreibung der Verarbeitungstätigkeit				
Bezeichnung der Verarbeitungstätigkeit	Zwecke der Verarbeitung *(gem. Art. 30 Abs. 1 lit. b DSGVO)*	Name des eingesetzten Verfahrens *(optionale Angabe)*	Beschreibung der Verarbeitungstätigkeit	Liegt eine Zweckänderung vor bzw. ist eine solche geplant? *(ja/nein)*
DigiExam				
DigiExam Allgemein ("Allgemein bedeutet hier auf alle Kategorien betroffener Personen gleichermaßen zutreffend")	täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation			nein
DigiExam Studierende	täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation			nein
DigiExam Aufsichtsführende	täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation			nein
DigiExam Dozierende	täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation			nein
DigiExam Account Manager	täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation			nein
DigiExam Admin	täuschungsfreie Durchführung von Online-E-Klausuren während der SARS-CoV-2-Krisensituation			nein

[redacted]

Neuanlage oder Änderung einer bestehenden Verarbeitungstätigkeit (VT)?

Ir

Neuanlage oder Änderung einer bestehenden Verarbeitungstätigkeit (VT)?			Innerorganisator Fachlicher Ansprechpartner		
Datum der Einführung	Datum der letzten Änderung	Datum der Beendigung	Abteilung / Funktion (Allgemeine Bezeichnungen ausreichend, Klarname kann genannt werden)	Telefon (Durchwahl Fachbereich ausreichend)	E-Mail-Adresse (allg. Bereichs-E-Mail-Adresse ausreichend)
20.05.2020	21.12.2020	-	E-Leanrning Didaktik Zentrum / [redacted]	+49 7361 576 [redacted]	canvas@hs-aalen.de
20.05.2020	21.12.2020	-	E-Leanrning Didaktik Zentrum / [redacted]	+49 7361 576 [redacted]	canvas@hs-aalen.de
20.05.2020	21.12.2020	-	E-Leanrning Didaktik Zentrum / [redacted]	+49 7361 576 [redacted]	canvas@hs-aalen.de
20.05.2020	21.12.2020	-	E-Leanrning Didaktik Zentrum / [redacted]	+49 7361 576 [redacted]	canvas@hs-aalen.de
20.05.2020	21.12.2020	-	E-Leanrning Didaktik Zentrum / [redacted]	+49 7361 576 [redacted]	canvas@hs-aalen.de
20.05.2020	21.12.2020	-	E-Leanrning Didaktik Zentrum / [redacted]	+49 7361 576 [redacted]	canvas@hs-aalen.de

ınerorganisatorische Ansprechpartner

Angaben zum ggf. mit dem Vera

ische Ansprechpartner					
ggf. technischer Ansprechpartner			Angaben zum ggf. mit dem Verantwortlichen ge *(gem. Art. 30 Abs. 1 lit. a D*		
Abteilung / Funktion (Allgemeine Bezeichnungen ausreichend, Klarname kann genannt werden)	Telefon (Durchwahl Fachbereich ausreichend)	E-Mail-Adresse (allg. Bereichs-E-Mail-Adresse ausreichend)	Name und Fachbereich	Straße	PLZ, Ort
Canvas Kernteam /		canvas@hs-aalen.de			
Canvas Kernteam /		canvas@hs-aalen.de			
Canvas Kernteam /		canvas@hs-aalen.de			
Canvas Kernteam /		canvas@hs-aalen.de			
Canvas Kernteam /		canvas@hs-aalen.de			
Canvas Kernteam /		canvas@hs-aalen.de			

ntwortlichen gemeinsam Verantwortlichen

Kategorien personenbezogener Daten

meinsam Verantwortlichen SGVO)			Kategorien personenbezogener Daten (gem. Art. 30 Abs. 1 lit. c DSGVO)		
Land	Telefon	E-Mail-Adresse	Kategorien betroffener Personen je personenbezogenem Datum	Beschreibung der Kategorien von personenbezogenen Daten	**Besondere** Kategorien personenbezogener Daten
			Allgemein	Geräte-/Hardware-Informationen E-Mail-Adresse, IP-Adresse, Vorname, Nachname, E-Mail-Adresse,	-
			Studierende	Bei Nutzung ohne Remote-Proctoring: Student-Code (i.d.R. E-Mailadresse), Prüfungseingaben, Bei Nutzung mit Remote-Proctoring zusätzlich: Video-, Audio- und Bildschirmdaten, Chateingaben + Informationen aus Teil "Allgemein"	Identifizierungsdokumente (Studierendenausweis, Personalausweis, anderes Ausweisdokument), Biometrische Daten (Gesichtserkennung) zum Abgleich
			Aufsichtsführende (und aufsichtsführende Dozierende, Admins)	Bei Nutzung mit Remote-Proctoring zusätzlich: Chateingaben Optional (bei direktem Kontakt mit Studierenden über Remote-Proctoring-Tool):	-
			Dozierende	Informationen aus Teil "Allgemein"	-
			Account Manager	Informationen aus Teil "Allgemein"	-
			Admin	Informationen aus Teil "Allgemein"	-

Rechtsgrundlage der Verarbeitungstätigkeit

Rechtsgrundlage der Verarbeitungstätigkeit *(vgl. Art. 5 Abs. 1 it. a DSGVO)*			Interne Empfänger (*(= Personen oder Stellen i*
Bezeichnung der Vorschrift(en) oder Hinweis auf Einwilligung	Rechtsgrundlage bei Zweckänderung *(wenn "ja" in Spalte F angegeben wurde)*	Erläuterung	Abteilung / Funktion *(KEINE Namen nennen)*
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 diesem Bild extrahiert	Aufsichtsführende, Dozierende, Admins
Landesbeamtengesetz BW (LBG) 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			Dozierende, Admins, Account Manager (teilweise)
Landesbeamtengesetz BW (LBG) 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			Admins, Account Manager (teilweise)
Landesbeamtengesetz BW (LBG) 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			Account Manager
Landesbeamtengesetz BW (LBG) 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			

Empfänger personenbezogener Daten *(gem. Art. 30 Abs. 1 lit. d und e DS-GVO)*					
Zugriffsberechtigte) *innerhalb der Hochschule)*	**Externe Empfänger** *(= Personen und Stellen, die nicht Teil der Hochschule sind)*			**Datenübermittlung in ein Drittland (= Land außerhalb EU/EWR) oder an eine internationale Organisation**	
Zweck	Empfänger bzw. Empfängerkategorie *(z.B. Finanzamt xy, Bank xy)*	Zweck bzw. Tätigkeit	Empfänger ist als Auftragsverarbeiter tätig	Findet eine entsprechende Datenübermittlung satt? *(ja / nein)*	Ist eine entsprechende Datenübermittlung geplant? *(ja / nein)*
	DigiExam Solutions Sweden AB	Anbieter des Diensts	ja	nein → weiter mit Spalte AT	nein → weiter mit Spalte AT
Aufsichtsführende, Dozierende: Durchführung der Prüfung,	DigiExam Solutions Sweden AB	Anbieter des Diensts	ja	nein → weiter mit Spalte AT	nein → weiter mit Spalte AT
Admins: Unterstützung der Durchführenden auf Anfrage Account Manager: Account verwalten	DigiExam Solutions Sweden AB	Anbieter des Diensts	ja	nein → weiter mit Spalte AT	nein → weiter mit Spalte AT
Admins: Unterstützung der Durchführenden auf Anfrage Account Manager: Account verwalten	DigiExam Solutions Sweden AB	Anbieter des Diensts	ja	nein → weiter mit Spalte AT	nein → weiter mit Spalte AT
	DigiExam Solutions Sweden AB	Anbieter des Diensts	ja	nein → weiter mit Spalte AT	nein → weiter mit Spalte AT
Rechte- und Accountverwaltung	DigiExam Solutions Sweden AB	Anbieter des Diensts	ja	nein → weiter mit Spalte AT	nein → weiter mit Spalte AT

Fristen für die Löschung der verschie

Externer Empfänger hat Sitz in Drittland hat oder ist eine internationale Organisation *Nur ausfüllen, wenn in Spalte AM oder AN die Antwort "JA" lautet*			
Empfänger hat Sitz in einem Drittland oder es handelt sich um eine internationale Organisation	Drittland oder Name der internationalen Organisation	Datenübermittlung findet wie folgt statt:	Rechtsgrundlage für Datenübermittlung:
-	-	-	LHG
-	-	-	LHG
-	-	-	LHG
-	-	-	LHG
-	-	-	LHG
-	-	-	LHG

Fristen für die Löschung der verschiedenen Datenka *(gem. Art. 30 Abs. 1 lit. d und e DS-GVO)* *→ Statt der Angaben kann ein Löschkonzept als Anlage beig*	
Kategorie der personenbezogenen Daten	Frist
	Siehe Anlage 4
	Siehe Anlage 4
	Siehe Anlage 4
	Siehe Anlage 4
	Siehe Anlage 4
	Siehe Anlage 4

:denen Datenkategorien		Klassifizierung des Risikos			Technische und organisatorische Maßnahı
tegorien *efügt werden*		Klassifizierung des Risikos ***Sofern die Frage nach dem Risiko mit "JA" beantwortet wird, muss eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO durchgeführt und als separate Anlage beigefügt werden.***			Technische und organisatorische Maßnahmen (TOM) *(gem. Art. 32 DS-GVO)*
Art der Löschung *(optionale Angabe)*		Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?	Risikoklasse	Erläuterung zur Eingruppierung in Risikoklasse	Allgemeine Beschreibung *(oder als Anlage beifügen)*
		Ja→ weiter mit Spalte AY	mittel	Siehe Anlage 10	Siehe Anlage 3
		Ja→ weiter mit Spalte AY	mittel	Siehe Anlage 10	Siehe Anlage 3
		Ja→ weiter mit Spalte AY	mittel	Siehe Anlage 10	Siehe Anlage 3
		Ja→ weiter mit Spalte AY	mittel	Siehe Anlage 10	Siehe Anlage 3
		Ja→ weiter mit Spalte AY	niedrig	Siehe Anlage 10	Siehe Anlage 3
		Ja→ weiter mit Spalte AY	mittel	Siehe Anlage 10	Siehe Anlage 3

men (TOM)

Hilfestellung zur Risikobewertung

Auswirkung aus Sicht des Betroffenen				
Maximal	4	8	12	16
Signifikant	3	6	9	12
Eingeschränkt	2	4	6	8
Vernachlässigbar	1	2	3	4
	Vernachlässigbar	Eingeschränkt	Signifikant	Maximal

Eintrittswahrscheinlichkeit

Drop-Downs

Übermittlung in Drittstaat
ja → weiter mit Spalte AO
nein → weiter mit Spalte AT

Löschfristen - Art der Löschung
automatisch
manuell

Zweckänderung
ja
nein

Risikoabschätzung
Nein → weiter mit Spalte BB
Ja→ weiter mit Spalte AY

niedrig
mittel
hoch

Datenname	Datenbeschreibung	Aufbewahrungsdauer	Quelle der Information	Anmerkung
Identifikationsdaten	Student-Code, Vorname, Nachname, E-Mailadresse	Löschung auf Anfrage der Hochschule (Data Controller) aus der primären Datenbank unmittelbar, aus den täglichen backups nach 90 Tagen und aus den Log Files und damit überall nach 180 Tagen. Hochschulseitig existiert eine Mindestspeicherfrist von vier Wochen bei erfolgter Rechtsmittelbelehrung (§ 70 VwGO) und von bis zu einem Jahr bei unterlassener Rechtsmittelbelehrung (§ 58 Abs. 2 VwGO). Gleiches gilt, sofern ein Widerspruchs- oder ein Klageverfahren gegen die Prüfungsbewertung noch nicht bestands- bzw. rechtskräftig abgeschlossen ist. In diesen Fällen tritt an die Stelle einer Löschung die Einschränkung (Sperrung) der personenbezogenen Daten.	Anlage 2 & Anlage 14	
Geräte-/Hardware-Informationen	IP-Adresse, MAC-Adresse, Domain-Adressen, Computer-Betriebssystem, approximierte Standortdaten, Metadaten	Löschung auf Anfrage der Hochschule (Data Controller) aus der primären Datenbank unmittelbar, aus den täglichen backups nach 90 Tagen und aus den Log Files und damit überall nach 180 Tagen. Hochschulseitig existiert eine Mindestspeicherfrist von vier Wochen bei erfolgter Rechtsmittelbelehrung (§ 70 VwGO) und von bis zu einem Jahr bei unterlassener Rechtsmittelbelehrung (§ 58 Abs. 2 VwGO). Gleiches gilt, sofern ein Widerspruchs- oder ein Klageverfahren gegen die Prüfungsbewertung noch nicht bestands- bzw. rechtskräftig abgeschlossen ist. In diesen Fällen tritt an die Stelle einer Löschung die Einschränkung (Sperrung) der personenbezogenen Daten. HTTP logs werden mit einer Aufbewahrungsfrist von 30 Tagen protokolliert.	Anlage 2, Anlage 13 & Anlage 14	
Informationen zur Beschäftigung	Berufsbezeichnung, Funktion, Name des Arbeitgebers	Löschung auf Anfrage der Hochschule (Data Controller) aus der primären Datenbank unmittelbar, aus den täglichen backups nach 90 Tagen und aus den Log Files und damit überall nach 180 Tagen. Hochschulseitig existiert eine Mindestspeicherfrist von vier Wochen bei erfolgter Rechtsmittelbelehrung (§ 70 VwGO) und von bis zu einem Jahr bei unterlassener Rechtsmittelbelehrung (§ 58 Abs. 2 VwGO). Gleiches gilt, sofern ein Widerspruchs- oder ein Klageverfahren gegen die Prüfungsbewertung noch nicht bestands- bzw. rechtskräftig abgeschlossen ist. In diesen Fällen tritt an die Stelle einer Löschung die Einschränkung (Sperrung) der personenbezogenen Daten.	Anlage 2 & Anlage 14	
(Prüfungs-) Aufzeichnungen	Video-, Audio- und Bildschirmdaten, Chateingaben	Liegt kein Verdacht einer Täuschung vor, so werden die Daten zwei Wochen nach dem jeweiligen Prüfungszeitraum gelöscht. Beim Verdacht einer Täuschung erfolgt die Löschung nach eindeutiger Feststellung eines Täuschungsversuchs. Spätestens aber vier Wochen nach Beendigung des Prüfungszeitraums aus der primären Datenbank, aus den täglichen backups nach 90 Tagen und aus den Log Files und damit überall nach 180 Tagen.	Anlage 3 & Anlage 14	

Risikomanagement

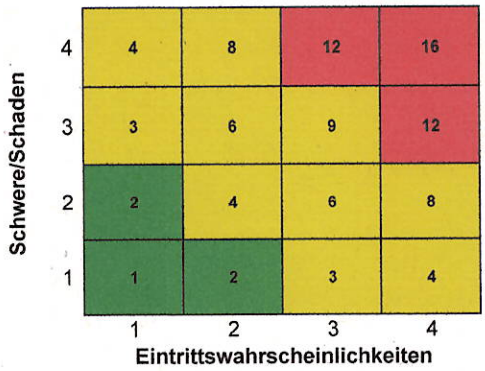
zum DSFA-Bericht

DigiExam

Inhalt:

Legende

1. Risikomatrix für die Indexierung der Risiken



Index	Bezeichnung Risikoindex
	geringes Risiko
	Risiko
	hohes Risiko

2. Eintrittswahrscheinlichkeit

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	Beispiel
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

3. Schwere/Schaden

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	Beispiel
1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.	**immateriell:** leichte Verärgerung **materiell:** Zeitverlust **physisch:** vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	**immateriell:** geringe, aber objektiv nachweisbare psychische Beschwerden **materiell:** deutlich spürbarer Verlust an privatem Komfort **physisch:** minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	**immateriell:** schwere psychische Beschwerden **materiell:** finanzielle Schwierigkeiten **physisch:** schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	**immateriell:** dauerhafte, schwere psychische Beschwerden **materiell:** erhebliche Schulden **physisch:** dauerhafte, schwere körperliche Beschwerden

Verfügbarkeit

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Verfügbarkeit	Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VB.1	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	IT-Fehlfunktion	Hard- und/oder Software-Fehlfunktion führen dazu, dass erforderliche digitale Daten unwiederbringlich verloren gehen.	Sehr gering, aber nicht auszuschließen	2	Schaden wäre überschaubar bis substanziell, da Prüfungsleistung nicht gewertet werden kann	3	6	Synchronisierung Online und Offline, Intervall <1min. bei nachweislichem technischen Fehler kann Prüfungsleistung nachgeholt werden	Eintrittswahrscheinlichkeit kann durch Synchronisierung und kurze Intervalle stark minimiert werden, die Schwere des Schadens kann durch Maßnahmen ebenfalls auf ein Minimum reduziert werden.	gr
VB.2	=VB.1	Interner Administrator	Interaktionen eines User mit weitreichenden Administratorenrechten mit DigiExam führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Fehlerhafte Bedienung unwahrscheinlich, da Admins geschult, aber nicht auszuschließen	2	Schaden wäre überschaubar bis substanziell, da Prüfungsleistung nicht gewertet werden kann	3	6	Admins können nur archivieren, nicht löschen	Admins der Hochschule können Klausuren nur archivieren, nicht löschen	gr
VB.3	=VB.1	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware gehen erforderliche Daten unwiederbringlich verloren.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Schaden wäre überschaubar bis substanziell, da Prüfungsleistung nicht gewertet werden kann	3	12	Basis Schadsoftware-/ Hackerabwehrsystem nutzen, Präventionsmaßnahmen durch Implementierung von Sicherheitsfunktion durch DigiExam und Sicherheitseinweisung der Nutzenden über die eventuellen Risiken	Durch ein aktuelles System können viele Angriffe verhindert werden und damit die Eintrittswahrscheinlichkeit verringert werden.	ge
VB.4	Der Anbieter kann die Bereitstellung der Daten nicht mehr gewährleisten	Anbieter	Anbieter geht Bankrott oder verliert Daten durch IT-Fehler	Unwahrscheinlich aber nicht ausgeschlossen, Redundanz und Backups sollen Verlust durch IT-Fehler verhindern	2	Klageverahren gegen Prüfungsbewertung, Speicherung von einem Jahr vorgeschrieben, Daten können jederzeit offine gespeichert werden	3	6	Rechtsgrundlage sichert ab	DigiExam muss im Falle der Insolvenz den der Hochschule Aalen die Prüfungsdaten / Personendaten zur Verfügung stellen [siehe Art. 13 DSGVO (1) c)]	gr

Vertraulichkeit

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Vertraulichkeit	Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VT.1	Personen können unmittelbar unbefugt auf DigiExam zugreifen	IT-Fehlfunktion	Aufgrund eines Hard- und/oder Softwarefehlers (z.B. Fehler in Berechtigungsmanagementfunktion) können Unbefugte auf die Daten in DigiExam zugreifen.	DigiExam wird auf dem neusten Stand gehalten und basiert auf modernen zuverlässigen Sicherheitsstandards. Aufgrund der bisherigen Erfahrungen ist eine IT-Fehlfunktion immer möglich, aber eher unwahrscheinlich.	2	Personen können unberechtigt an vertrauliche Daten gelangen.	3	6	DigiExam wird durch automatische Updates auf dem neusten Stand der Technik gehalten, um Fehler zu vermeiden	Durch regelmäßige automatische Updates kann das Risiko eines Softwarefehlers minimiert werden.	ge
VT.2	=VT.1	Internes Personal	Das Rollen- und Berechtigungskonzept weist Fehler auf	Bei Personalwechsel werden Berechtigungen nicht sofort geändert / entzogen. Bei häufigem Personalwechsel durchaus Möglichkeit dass keine rechtzeitige Aktualisierung des Rollensystem statfindet.	2	Beschäftige der Hochschule sind zur Verschwiegenheit und zur Meldung solcher Fehlfunktionen verpflichtet.	1	2	zentrale Verwaltung Internes Personal muss Verpflichtung zur Einhaltung des Datenschutzes unterschrieben haben	Komplexität des Berechtigungskonzeptes ist niedrig, daher Häufigkeit für Fehlerszenario (kein rechtzeitiges aktualisieren) gering	gr
VT.3	=VT.1	Interner User mit erweiterten Zugriffsrechten auf DigiExam	Beim Verlassen des Arbeitsplatzes wird dieser nicht gesperrt, so dass andere Personen unbefugt Einblick in DigiExam-Daten erhalten können.	Das Sperren des IT-Arbeitsplatzes beim Verlassen ist noch nicht zur Selbstverständlichkeit geworden.	2	Nur Einsicht in Daten führt noch zu keinem erheblichen Schaden.	2	4	Beschäftigte durch Dienstanweisung sensibilisieren Internes Personal muss Verpflichtung zur Einhaltung des Datenschutzes unterschrieben haben Richtlinie Sperrung nach bestimmer Zeit	Durch Maßnahmen zur Sensibilisierung sowie Richtlinien zur Sperrung der Arbeitsplätze kann die Eintrittswahrscheinlichkeit minimiert werden.	gr
VT.4	=VT.1	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware wird unbefugt auf die Daten zugegriffen.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Personen können unberechtigt an vertrauliche Daten gelangen und diese missbrauchen. Die Kenntnisnahme krimineller Dritter kann zu weiterführenden Unanehmlichkeiten der betroffenen Person(en) führen.	4	16	Basis Schadsoftware-/ Hackerabwehrsystem nutzen, Präventionsmaßnahmen durch Implementierung von Sicherheitsfunktion durch DigiExam und Sicherheitseinweisung der Nutzenden über die eventuellen Risiken	Durch ein aktuelles System können viele Angriffe verhindert werden und damit die Eintrittswahrscheinlichkeit verringert werden.	ge
VT.5	=VT.1	Böswilliger Interner User	Personal kann an vertrauliche Daten gelangen und diese missbrauchen.	Nicht auszuschließen, nach bisherigen Erfahrungen aber noch nie eingetreten	2	Personen können an vertrauliche Daten gelangen und diese missbrauchen (trotz unterschriebener Verpflichtung zum Datenschutz)	4	8	Internes Personal muss Verpflichtung zur Einhaltung des Datenschutzes unterschrieben haben	Risiko kann nicht minimiert werden.	ge

Datenintegrität

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Datenintegrität	Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
DI.1	Digitale Daten werden fehlerhaft oder unzulässig verändert	Böswilliger interner User	Interne Systembenutzer verändern vorsätzlich fehlerhaft oder unzulässig Daten.	In der Vergangenheit konnte kein solch vorsätzliches Verhalten aufgedeckt werden. Der Interne User hat anhand der verteilten Nutzungsrechte keine Möglichkeit Daten fehlerhaft oder unzulässig zu verändern	1	manipulierte Prüfungsbewertung kann schwerwiegende Folgen für die betroffene Person haben	4	4	Prüfungseinsicht Nachvollziehbarkeit der Änderungen an Prüfungsbewertungen	Durch Prüfungseinsicht und Nachvollziehbarkeit der Änderungen kann die Schwere des Schadens stark reduziert werden.	gr
DI.2	=DI.1	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware werden Daten fehlerhaft oder unzulässig verändert (z.B. externe Datenverschlüsselung durch Ransomware).	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist. Auch wenn an der Hochschule selbst bisher keine Erfahrungen mit gezielten Hackerangriffen gemacht wurden, ist die Eintrittswahrscheinlichkeit dennoch hoch.	3	Das Änderungspotenzial von cyberkriminellen Angriffen umfasst auch unerwünschte Massendatenänderungen mit den daraus folgenden Auswirkungen.	4	12	Basis Schadsoftware- / Hackerabwehrsystem nutzen Basis Backup-Struktur nutzen Verschlüsselung der Daten Sicherheitskonzept des Rechenzentrums	Trotz der ergriffenen Maßnahmen für die aktive und passive Risikobewältigung kann das Risiko nur in den gelben Bereich gebracht werden.	ge

Glossar

Begriff/Abkürzung	Erläuterung
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 Dateninteg-rität des SDM-Gewährleistungsziels Integrität.

Zielerfüllungsmanagement

zum DSFA-Bericht

DigiExam

Inhalt:

Legende

Ergebnis der Gefährdungsbewertung

Index	Bezeichnung Gefährdungsindex
	Keine Gefährdung, d.h. prognostizierte Vollerfüllung des betrachteten Ziels
	Es kann von einer kontinuierlichen Vollerfüllung des Ziels vertretbar ausgegangen werden. Gleichwohl kann eine Gefährdung des Ziels nicht ganz ausgeschlossen werden.
	Unzureichendes Schutzniveau für das betrachtete Ziel

Datenminimierung

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Datenminimierung	Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.	gr

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
DM.1	Nicht erforderliche Personaldaten erfasst / übermittelt (Studentcode ist Matrikelnummer)	Konfiguration	Verknüpfung in andere Systeme bei denen Matrikelnummer verwendet wird	Durch eine ungeeignete Konfiguration werden mehr Daten übermittelt als notwendig.	gr	Die E-Mailadresse kann ebenfalls als Identifizierung der Studierenden genutzt werden. Somit entfällt ein zusätzliches Datum.	Die Gesamtmenge der Daten wurde minimiert.	gr

Intervenierbarkeit

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Intervenierbarkeit	Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.	ge

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
IV.1	Geltend gemachte Auskunftsansprüche können nicht oder nicht rechtzeitig erfüllt werden.	Internes Personal	Ein ordnungsgemäß geltend gemachter Auskunftsanspruch wird nicht oder nicht rechtzeitig erfüllt.	Durch Canvas-Kernteam können Auskunftsersuche in diesem Bereich fristgerecht beantwortet werden. Trotzdem kann es zu Verzögerungen im Arbeitsablauf kommen, die eine fristegerechte Auskunft verhinden.	ge	Direkte Zuständigkeit für Auskunftsansprüche zuweisen	Bei direkte Zuständigkeit Wahrscheinlichkeit für eine nicht fristgerechte Antwort minimiert.	gr
IV.2	Geltend gemachte Löschansprüche können nicht oder nicht rechtzeitig erfüllt werden.	Internes Personal / DigiExam	Ein ordnungsgemäß geltend gemachter Löschanspruch wird nicht oder nicht rechtzeitig erfüllt.	Löschansprüche werden bearbeitet und ggf. an DigiExam weitergeleitet.	ge	Löschkonzepte / Löschfristen DigiExam vertraglich festhalten, enge Kommunikation mit DigiExam um schnelle Ausführung des Anspruchs zu gewährleisten	DigiExam ist vertraglich verpflichted Löschfristen und Löschkonzepte einzuhalten	gr
IV.3	Datenverarbeitung ohne Einwilligungserklärung	Internes Personal / Prüfungsamt	Teilnahme an Prüfung ohne Einwilligung (Verarbeitung von Daten ohne Einwilligung)	Keine Rechtsgrundlage zur Verarbeitung, Fehler bei Einpflegung der Einwilligungen / Erstellung der Prüfungslisten durch menschliche Fehler wahrscheinlich.	ro	Anmeldung mit Einwiliigung oder Information über Schreiben an der Hochschule mit personeller Aufsicht gekoppelt. Aufsicht prüft die Prüfungslisten.	Durch Prüfungsliste ist dann bekannt, welche Daten verarbeitet werden dürfen und welche nicht. Durch doppelten Check der Liste kann Risiko einer nicht rechtmäßigen Verarbeitung ohne Einwilligung minimiert werden	ge

Transparenz

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Transparenz	**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**	ge

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
TP.1	Der Grundsatz der Transparenz kann nicht lückenlos gewährleistet werden.	Internes Personal	Die normativen Mindestinhalte der erforderlichen Information werden betroffenen Personen nicht bereitgestellt.	Die rechtskonforme inhaltliche Umsetzung der Informationspflicht bzgl. des Prozesses "DigiExam" ist unzureichend.	ro	Regelmäßiger (technsicher) Austausch mit DigiExam.	Regelmäßiger Austausch mit DigiExam, Überprüfung der bestehenden Informationen auf Vollständigkeit. Kommunikation auf technischer Ebene erhöht Wahrscheinlichkeit, dass fehlende Informationen entdeckt werden.	ge
TP.2	= TP.1	Internes Personal	Informationen zu DigiExam sind nicht leicht zugänglich und/oder nicht hinreichend verständlich.	Insbesondere die juristischen Formulierungsgepflogenheiten ("Behördendeutsch") und die Komplexität der Verarbeitung können zu einer schweren Verständlichkeit führen.	ge	Infoschreiben, Informationskurse, Infoveranstaltungen, Ansätze Informationen verständlich und auf Behördendeutsch verzichtend darzustellen	Es wird Wert darauf gelegt Informationen so verständlich und zugänglich wie möglich bereitzustellen. Trotzdem kann auf eine gewisse Komplexität nicht verzichtet werden	ge

Nichtverkettung

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Nichtverkettung	**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**	ge

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
NV.1	Daten können durch den Einsatz von integrativen IT-Systemen zusammengeführt werden.	~ Internes Personal ~ IT-Fehlfunktion	Durch hochintegrative Systeme werden verschiedene Daten zusammengeführt und können rechtswidrig verarbeitet werden (z.B. wegen Lücke in Berechtigungskonzept oder technischer Fehler bei Berechtigungssteuerung). Canvas Admins haben fakultätsübergreifenden Zugriff.	Hinsichtlich der bestehenden Komplexität integrativer IT-Systeme sind unbeabsichtigte Konfigurationslücken und technische Fehler bei der Berechtigungssteuerung als Gefährdung für die Erfüllung der Nichtverkettung einzuschätzen.	ro	Rollen- und Berechtigungskonzept	Zugriff auf DigiExam wird auf Fakultät begrenzt, zuständiges Personal kennt die Vorgänge in der jeweiligen Fakultät.	ge
NV.2	Daten können durch unbefugte Datenweitergabe zusammengeführt werden.	Internes Personal	Personal, das an DigiExam beteiligt ist, gibt rechtswidrig Daten für eine andere Verarbeitung weiter.	Personal das mit DigiExam arbeitet kann durch Dritte leicht veranlasst werden, Daten nicht normenkonform weiterzugeben.	ro	Benutzer schulen Rollen- und Berechtigungskonzept umsetzen, Dienstanweisung für die Übermittlung personenbezogener Daten umsetzen	Vertretbares Schutzniveau ist hergestellt. Vereinzelte, nicht kontrollierbare Weitergaben (z. B. mündliche Weitergabe bei Mitarbeitertreffen) können nicht ausgeschlossen werden.	ge
NV.3	Daten können durch überschneidende Aufgabenbereiche zusammengeführt werden.	Interne Organisations-verantwortung	Personal,das parallel in verschiedenen Bereichen gleichzeitig arbeitet, führt rechtswidrig Daten aus mehreren Bereichen zusammen.	Dem Personal, das gleichzeitig in zwei Bereichen arbeitet, fällt es oft sehr schwer, die Bereiche den normativen Anforderungen entsprechend abzugrenzen.	ge	Rolle muss explizit gewechselt werden	Hat eine Person Zugriff auf mehrere Bereiche muss für den entsprechenden Bereich jeweils eine Rolle ausgewählt werden.	gr

Konzeptionseinhaltung

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Konzeptionseinhaltung	**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**	ge

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
KE.1	Das konzepierte Soll weicht von der umgesetzten Verarbeitung (Ist) ab	Internes Personal	Der Nachweis einer ordnungsgemäßen Verarbeitung kann nicht erbracht werden.	Das Risiko, dass dokumentierte Konzeption und Umsetzung auseinanderlaufen, ist hoch.	ro	regelmäßige Schulungen und Überprüfung	Durch regelmäßige Prüfungen und Schulungen kann das Risiko, dass das konzepierte Soll von der umgesetzten Verarbeitung abweicht minimiert werden.	ge
KE.2	= KE.1	IT-System	DigiExam nimmt Änderungen vor, die die Erfüllung der dokumentierten datenschutzrechtlichen Anforderungen gefährden.	Eine solche Änderung ist unwahrscheinlich, da DigiExam an die DSGVO gebunden ist.	gr	Die Gefährdungsquelle wird auf rechtlicher Ebene kontrolliert, weitere Maßnahmen sind nicht nötig.	Die Gefährdung ist gering.	gr
KE.3	= KE.1	Internes Personal	Die vorgegebenen Maßnahmen werden nicht eingehalten.	Bei manuellen Prozessen unterlaufen Fehler.	ro	Entscheidende Vorgänge werden zentral verwaltet	Durch eine deutliche Reduktion der Fehlerquellen kann die Gefährdung als gering eingeschätzt werden.	gr

Richtigkeit

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Richtigkeit	Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.	gr

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
RI.1	Es werden unrichtige Daten verarbeitet	Internes Personal	Unrichtige Daten, deren Verarbeitung nach dem Datenschutz untersagt ist, werden verarbeitet.	Von Beschäftigten gemachte Angaben waren in der Vergangenheit manchmal (selten!) nicht zutreffend. Zudem führen insbesondere versehentliches Verschreiben oder Verwechslung zu unrichtigen Daten.	ge	Zentrale Nutzerverwaltung	Durch eine zentrale Nutzerverwaltung können Risikoquellen minimiert werden.	gr
RI.2	=RI.1	Software-Fehler	Unrichtige Daten, deren Verarbeitung nach dem Datenschutz untersagt ist, werden verarbeitet.	Fehler bei Übertragung / Verarbeitung ist durch aktuelle Software sehr unwahrscheinlich, kann aber nicht ausgeschlossen werden	ge	Durch ein regelmäßiges automatisches aktualisieren wird die Software auf dem neusten Stand gehalten, was Fehler bei der Datenübertragung stark minimiert.	Durch aktuelle Software kann die Gefährdungsbewertung in den grünen Bereich gebracht werden.	gr

Glossar

Begriff/Abkürzung	Erläuterung
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-Schutzbedarfsziele	Davon umfasst sind die vier SDM-Gewährleistungsziele Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung sowie der Teilzielaspekt Konzeptionseinhaltung und Richtigkeit des SDM-Gewährleistungsziels Integrität.