Standard Contractual Clauses (SCCs)

Data Processor Agreement

- Controller to Processor

Ver. July 2024

WISEflow

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the

controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679/.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I: LIST OF PARTIES

Controller(s):
Name (Institution):

Address:

Contact person's name, position, and contact details:

Data protection officer:

Signature:

Date:

Processor(s):
Name:

Address:

Contact person with responsibility for data protection:

Contact person with responsibility for the agreement:

Signature:

Date:

These Standard Contractual Clauses and Data Protection Agreement are liable to Danish Law and Datatilsynet as Denmarks Supervisiory Authority.

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is transferred:

- The Controller's students, applicants, or similar assessment participants (including temporary or casual participants).
- The Controller's employees working as managers, assessors, authors, supporters or similar (including temporary or casual staff).
- Authorised Users, Affiliates and other participants from time to time to whom the Controller has granted the right to access the Services in accordance with the terms of the Agreement.

Categories of personal data transferred:

- **Identity Data** including first name, maiden name, last name, student id, username or similar identifier.
- **Contact Data** including email address and telephone number.
- **Educational and professional data** including assignments, submission, grades, marks, results, and feedback, that may carry personal information.
- **Monitoring data** including screen capturing of participants screens during exam as well as their active application processes on their used computer during exam.
- **Technical Data** including internet protocol (IP) address.
- **Usage & log Data** including information about how the data subject uses the Services.

Sensitive data transfer (if applicable):

- **Identity Data** including Civil registration number of Authorised Users (if applied)
- **Biometric data** (if applied) including Visual (face comparison) and audio (voice detection) data of Authorised Users. Biometric data is processed and stored at Amazon S3 in EU (Germany/Ireland). Data is only processed for authentication and monitoring purposes in relation to the exam session and is not shared with third party. The data importer has a default stricter data retention policy of 6 month for automatic deletion of biometric data, but the data controller can request deletion prior to this.
- Access to Biometric data is restricted to only authorised personnel at UNIwise and requires personal two factor authentication.

The frequency of the transfer:

- Data is transferred on a continuous basis.

Nature of the processing:

- Personal Data will be processed to the extent necessary to provide the Services in accordance with both the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller.
- Processing operations include but are not limited to: management, authoring, participation, invigilation, monitoring and assessment and marking of students, applicants, or similar exams and assessments. This operation relates to all aspects of Personal Data processed.
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Services and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.
- Virus, anti-spam and Malware checking in accordance with the Services provided. This operation relates to all aspects of Personal Data processed.
- URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Agreement.

Purpose(s) of the data transfer and further processing:

- The purpose of the processing is the provision of Services by the Processor to the Controller under the Agreement and includes but a not limited to:
    - Workflow support for institutions to carry out exams and assessments, i.e. role based

assistance for exam and assessment authors, managers, supporters, invigilators, markers and assessors and participants.
- Support for carrying out various exam and assessment formats, i.e. onsite, remote, lockdown, monitored, MCQ, oral, essay, portfolio, timed etc. forms of exams and assessments relevant at educational institutions.
- Providing security in and around conducting exams and assessment to secure authenticity of relevant persons and participants as well as monitoring and preventing misconduct when participants do exams and assessments.
- Storing and archiving exams and assessment assignments, submissions and attachments together with relevant workflow and log data.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

- The duration of the processing corresponds to the duration of the Agreement.
- Subject to this, the data processor shall on an ongoing basis delete data that are more than 2 years old, unless the data controller has chosen to opt in on extending the retention and thus instructed the data processor to persist their data and not to delete it after 2 years.
- Subject to this, the data processor shall in any event delete all Production Data including Personal Data in its systems within 3 months of the effective date of termination of the Agreement.
- Personal Data of the data controller, which is stored in backups and log data in the system shall be deleted within 1 year of the effective date of termination of the Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

- Subject matter and nature for transfers to sub processors are described in Annex IV. The duration of the processing corresponds to the duration of the Agreement.

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

UNIwise is exercising a comprehensive and methodical IT Security scheme of policies, process description, access controls, risk management and documentation following international standard framework of ISO 27001. Our IT Security Policy describes in further detail the general technical and organisational measures under which we as a data processor and supplier of our exam platform WISEflow, securely operate, store, develop and maintain the platform to those standards. Our IT Security framework and how we adhere to it are annually audited by an external party. Upon request UNIwise can provide a copy of the most recent sanctioned IT Security Policy. Any IT Security Policy or documentation hereof submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

UNIwise is currently ISAE 3402 certified and will continue to maintain these certifications and/or other substantially similar or equivalent certifications for the term of the Agreement. The technical and organisational measures defined herein are implemented on the basis of the international standard ISO 27001 and ISO 27018. UNIwise shall maintain controls materially as protective as those provided in the ISO 27001 and ISO 27018 or other substantially similar or equivalent certification requirements.

UNIwise utilises third party data centres that maintain ISO 27001, SOC 1, SOC 2 and SOC 3 certifications. UNIwise will not utilise third party data centres that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations. All platform data is stored within EU and UNIwise utilise multi-factor authentication on all accounts, together with detailed security measures described below.

UNIwise shall provide the Controller upon request a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

The following descriptions provide in its first part a general overview of the technical and organisational security measures implemented (1-8), and secondly a detailed technically specific account of measures – many in relation to our use of AWS (A-I). It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available, however additional information regarding technical and organisational measures may be found in UNIwise's IT Security Policy. It's acknowledged and agreed that the IT Security Policy and the technical and organisational measures described therein will be updated and amended from time to time, at the sole discretion of UNIwise. Notwithstanding the foregoing, the technical and organisational measures will not fall short of those measures described in the IT Security Policy in any material, detrimental way.

Our 8 general data security measures:

1. Entrance Control

Technical or organisational measures regarding access control, especially regarding legitimation of authorised persons:

Entrance control is in place to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to security requirements, business premises are monitored by security personnel. Access for employees is only possible with personal key. All other persons have access only after having identified themselves (e.g. at the main entrance).

2. System Access Control

Technical and organisational measures regarding the user ID and authentication:

System access control is in place to prevent unauthorised use of data processing systems used for the processing of Customer Data.

Remote access to the data processing systems is only possible through the Processor's secure VPN tunnel. When the user first tries to authenticate through the secure VPN tunnel, authorisation is only executed by providing a unique user name and password to a centralised directory service. All access attempts, successful and unsuccessful are logged and monitored.

Additional technical protections are in place using firewalls and proxy servers and state of the art encryption technology is applied where appropriate to meet the protective purpose based on risk.

3. Data Access Control

Technical and organisational measures regarding the on-demand structure of the authorisation concept, data access rights and monitoring and recording of the same:

Data access control is in place so data can only be accessed for which an access authorisation exists and data cannot be read, copied, changed or deleted in an unauthorised manner during the processing and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.

To maintain data access control, state of the art encryption technology is applied to the Personal Data itself were deemed appropriate to protect sensitive data based on risk.

4. Transmission Control

Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Personal Data on data media (manually or electronically).

Transmission control is implemented so that Personal Data cannot be read, copied, changed, or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which recipients a transfer of Personal Data is intended.

The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or Customer Data are detailed in the Security Policy. This standard includes a description of the protection required during the processing of data, from the creation of such data to deletion, including the protection of such data in accordance with the data classification level.

For the purpose of transfer control, an encryption technology is used. The suitability of an encryption technology is measured against the protective purpose.

The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred to companies located outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the Standard Contractual Clauses.

5. Data Entry Control

Technical and organisational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review.

System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

6. Data Processing Control

Technical and organisational measures to differentiate between the competences of principal and contractor:

Data processing control is in place to provide that Personal Data is processed by a commissioned data processor in accordance with the Instructions of the principal.

Details regarding data processing control are set forth in the Agreement and DPA.

7. Availability Control

Technical and organisational measures regarding data backup (physical/logical):

Data is stored in triplicate across 3 data centres, with 3 separate cross connections. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protect Personal Data against accidental destruction and loss.

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

8. Separation Control

Technical and organisational measures regarding purposes of collection and separated processing:

Personal Data used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.

Customer Data is stored in a way that logically separates it from other customer data.

<u>Our 9 technically specific data security measures (in the following we (UNIwise) is referred to as the controller):</u>

A. Pseudonymization

- UNIwise never uses real data for test purposes.
- Only internal ID's are used for reference in the service.

B. Encryption

- UNIwise uses the encryption options provided by AWS
- Use of the AWS KeyManagementSystem (KMS), which is FIPS 140-2 level 2 (parts to Level 3) certified
- AWS employees do not have access to customer keys or data.

- AWS NITRO EC2 instances are used where EBS volumes are AES 256 encrypted and the keys in the NITRO hardware are protected from unauthorized access, including from third parties.

C. Ensuring confidentiality

- UNIwise uses the AWS Identity and Access Management (IAM) Service to control access to, the AWS Service it uses and data it stores, e.g. stored objects, instances, subnets, configuration parameters at the technical (non-technical) level, API interfaces, etc.
- Only services from AWS European regions are used by the controller.
- The Global Route53 (Domain Name System (DNS) -) processes name resolution requests and only routes traffic to IP addresses configured by the Controller
- The IAM Global Service is used by UNIwise in such a way that no personal data is processed. (SAML, Federation, tokenized account, temporary account)
- Personal data at rest is AES 256 encrypted with a key managed by UNIwise.
- Data in Transit is encrypted using TLS 1.3, utilizing certificates managed by UNIwise in AWS Certificate Manager. Internal traffic is encrypted using TLS 1.3 Cipher suite: TLS_CHACHA20_POLY1305_SHA256 & External traffic is TLS 1.3 SHA256withRSA 2048 bit key size.
- Only services that support that support the ability to Encrypt, delete and monitor processing of personal data are used.
- Only services that have been tested according to the Cloud Computing Compliance Catalogue (C5) standards are used.
- UNIwise's internal operational policies define that: AWS Support requests are only made against instances of the test environments in which no personal data is located.
- For the systems with production data, UNIwise does not require AWS support at the data or customer system level.
- AWS NITRO EC2 instances are used to prevent all administrative access (including access by Amazon employees).
- AWS NITRO EC2 Graviton2 instances are used whose memory is permanently encrypted by 256 bits, preventing the physical reading of plaintext data in DRAM.
- UNIwise remains the owner of their content and can choose which AWS services can process, store, and host their content. AWS never accesses or uses their content without first asking permission. AWS never uses customer content for marketing or advertising purposes or derives information from it.
- UNIwise's use of AWS is governed by EU-US. Data Privacy Framework, where the EU Commission concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework.

D. Ensuring integrity

Integrity is ensured by the following measures:

- Only IAM based and authorised access is allowed (authentication and authorisation)
- The Controller implements IAM based access control policies based upon the need to know principle
- MD5 hash computation is implemented to combat technical integrity loss using the replication logic implemented in S3, including automatic and regular integrity checks.
- Encryption of the objects technically prohibits unauthorized modification.

E. Ensuring availability

- AWS commits to the following SLAs for the availability of each AWS service in a region to the controller: https://aws.amazon.com/legal/service-level-agreements/.
- UNIwise uses infrastructure in the AWS Dublin and Frankfurt Region and all three existing availability zones of each region, which is also taken into account in its application architecture.

This gives it very high resilience against individual component failures, up to the level of two entire data centers. In addition, the following options are used by UNIwise.

- Automate EBS Snapshots with Amazon Data Lifecycle Manager
- Maintain fleet functionality and availability with Amazon EC2 Auto Scaling
- Distribute incoming traffic across multiple instances in a single

F. Ensuring the resilience of system and services

- By using AWS services such as autoscaling and load balancing, UNIwise ensures that processing is stable even under heavy loads.

G. Available measure to restore personal data and access in the event of a physical or technical incident

- UNIwise implements back-ups based upon the RTOs and RPOs required to meet the data protection and availability needs of their business/service. UNIwise uses AWS tools such as snapshot for Elastic Block Storage (EBS) and Elastic Compute Cloud (EC2) to meet their requirements.

H. Measures to ensure effectiveness of measures

- As evidence of AWS TOMs, the CSP will provide an updated C5 attestation, as well as a review of the effectiveness of ISO 27018, as shown in the SOC 2 six-monthly privacy report.
- UNIwise implements CloudTrail, to provide an audit history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

I. Documentation on available measures

Order Processing Contract:

- AWS's AWS GDPR Data Processing Addendum (DPA) is part of the contract with UNIwise. The Standard Contractual Clauses are part of the DPA.

Data protection assurance:

- Valid certification against ISO 27018 Code of Conduct for the Protection of Personal Data in Public Clouds. https://aws.amazon.com/compliance/iso-27018-faqs/
- The effectiveness of ISO 27018 controls is tested twice a year and shown in the SOC 2 Data Protection Report. https://aws.amazon.com/compliance/soc-faqs/
- As a provider of cloud infrastructure services in Europe, AWS adheres to the Code of Conduct of Cloud Infrastructure Services Providers in Europe (CISPE). https://aws.amazon.com/compliance/cispe/
- AWS TOMs are assessed annually and reported in the C5 attestations repot https://aws.amazon.com/compliance/bsi-c5/

Proof of CSP IT Security: https://aws.amazon.com/compliance/services-in-scope/

- Valid certifications against ISO 27001, 27017, 27018, ISO 9001, PCI and other standards https://aws.amazon.com/compliance/programs/.
- AWS is supervised by BSI as Critical Infrastructure Operator in accordance with Industry Specific Standard (B3S).
- AWS follows internal IT security processes, that are tested under numerous compliance programs, such as System and Organization Controls (SOC).
- FIPS 140-2 Certification of the KMS.
- Verification of the crypto function of the NITRO Security card by the National Institute of Standards and Technology.
- Verification of the crypto function of the associated Linux kernel in the NITRO security card by the National Institute of Standards and Technology.

Data Protection Training at CSP:

- Employees undergo annual data protection training: C5 Attestation HR-03: Security Training and Awareness-raising Program
- According to the C5 Report 2018, an appropriate internal policy is available: “AWS Internal Privacy Policy”

ANNEX IV: LIST OF SUB-PROCESSORS

Sub-processor identity	Hosting location	Service	Purpose	Note	Contractual Safeguard	Website
AWS Amazon	Germany & Ireland	Data Hosting & Technology Service Provider	Support for cloud-based hosting and use of various servers, applications, databases, advanced services, storage and infrastructure setup, in order to provide a robust and scalable WISEflow for all institutions and users.	AWS services in use: • AppStream • CloudFront • CloudTrail • CloudWatch • Elastic Compute Cloud • Elastic Container Service • Elastic load Balancing • GuardDuty • Key Management Service • Recognition • Relational Database Service • Route 53 • Secrets Manager • Security hub • Simple Email Service The services are integrated and the foundation of WISEflow, all hosted within EU. All services comply with C5 (Cloud Computing Compliance Catalogue). Data including personal data is transferred automatically and encrypted using Key Management Service, rendering key access impossible for AWS. MD5 & timestamps are used and AWS are prohibited in processing any data themselves – including the purpose of enhancement of services.	DPA (SCC) under the EU - US data privacy framework	https://aws.amazon.com/compliance/data-privacy-faq/
Learnosity	Ireland	Authoring & Advanced Question	Support for providing authoring and rendering of MCQ and advanced	The service is integrated into WISEflow via Learnosity API's. Data is transferred	DPA	https://learnosity.com/platform/privacy/

		Technology Provider	questions inside WISEflow, in order for faculty to create MCQ based test, taken by participants.	automatically and encrypted, but only using internal ID's. No personal data is transferred and processed.		
Sentry (Functional Software Inc.)	Germany & United States* *) Service data is stored and processed in the region selected by the customer (in our case EU, Frankfurt). However, in some edge cases it may also be processed in the US.	Error tracking & Monitoring	To detect and remediate errors in WISEflow	Sentry distinguishes between Customer data and Service data, customer data is data about UNIwise as a client, i.e. users on the platform, billing details etc. Service data is the data that is logged to Sentry, and which may contain PII of WISEflow users, such as names, e-mails, IP addresses and the like. Service data is set to only be processed in EU (Frankfurt) region. Sentry has obtained the following compliance certifications: • SOC2 Type I • SOC2 Type II • HIPAA Attestation • ISO 27001	DPA (SCC) under the EU - US data privacy framework	https://sentry.io/legal/dpa/ The sentry DPA allows for them to generally process data in any location. Currently the only store and process data in Germany and the US. New subprocessors can be added by Sentry with 30 days notice. In case a new sub processor is added that is not in the EEA, US or a Safe third country, UNIwise will stop the usage of Sentry.
CloudFlare Inc.	Multiple locations	Caching of static resources, DDOS protection & Web application Firewall	Protecting integrity, confidentiality and availability of the data subject's personal data stored and processed in the WISEflow Originality platform, by providing DDOS protection and acting as Web Application Firewall to filter out malicious requests to the WISEflow servers.	With Cloudflare, data can be processed outside of the EEA, if the user of the WISEflow platform makes requests from a location outside of the EEA. For data processed in: • Andorra, • Argentina, • Canada, • Faroe Islands, • Guernsey, • Israel, • Isle of Man, • Japan,	DPA (SCC) under the EU - US data privacy framework	https://www. cloudflare.com/cloudflare-customer-dpa/

				• Jersey, • New Zealand, • Republic of Korea, • Switzerland, • United Kingdom, • Uruguay. The legal basis for the transfer is the adequacy decisions adopted by the European Commision for those countries. For transfers to the United States the legal basis for the transfer is Cloudflare's participation in, and self-certification to, the EU-US Data Privacy Framework. For all other third countries the legal basis for the transfer of personal data is EU's Standard Contractual Clauses including supplementary measures as necessary.		
Sub-processors outside WISEflow						
Brevo	France	Email Delivery Provider	Support for sending out release notes, announcement, and news to users, provided outside WISEflow in order to communicate WISEflow related news.	The service sits outside WISEflow and only target institution-appointed and self-subscribed users. No automatic data transfer is conducted between WISEflow and Brevo. Personal data (name and email) is processed only for those users appointed, or self-subscribed.	DPA	https://www.brevo.com/gdpr/
Zendesk	EEA	Customer Support Ticket Technology Provider	Support for 2nd level ticketing and support service provided outside WISEflow, in order to service WISEflow license administrators and supporters with	The service sits outside WISEflow and is only accessible for the appointed users pr. Institutions. No automatic data transfer is conducted between WISEflow and Zendesk. Data is	DPA (SCC) under the EU - US data privacy frame work	https://www.zendesk.com/company/privacy-and-data-protection/#ccpa

			help, questions and incidents. Link to service provided inside WISEflow.	encrypted in transit and at rest via AWS, and making it impossible for any "government authorities to circumvent its security measures to gain access to Service Data". Personal data (name and email) is processed only for those users appointed, or in the case where institutions themselves chose to disclose any personal data within a ticket. Users are recommended only to disclose internal ID for support processing.		
Hubspot	EEA	CRM Platform Provider	Support for handling sales, renewals and support services.	The service sits outside WISEflow and only target institution-appointed users. No automatic data transfer is conducted between WISEflow and Hubspot.	DPA (SCC) under the EU - US data privacy frame work	https://legal.hubspot.com/jst-europe
Feature-specific Sub-processors						
Geogebra	Austria	STEM based Question Technology Provider	Support for using special STEM related questions and Items inside WISEflow, but authored outside WISEflow using Geogebra.	The service is rendered inside WISEflow and is provided via integration. Only applicable if separate access to the service is acquired by customer. No personal or identifiable data is transferred.	DPA	https://www.geogebra.org/privacy

DRATA

Policy version history

Policy details

Policy name

Data Processing Agreement, WISEflow - English

Renewal date

October 6, 2026

Description

DPA for WISEflow in English.

Version history

Version 1

Creation date	Approval date	Published date	Owner	Approver(s)	Publisher
October 6, 2025	October 6, 2025	October 6, 2025	Sune Kjærgård	Sune Kjærgård	Sune Kjærgård