Personal Data Processing Agreement

between

Personal Data Controller, [Customer name],

Incorporated in [country], [company number] with registered address at [address] (“the Controller”)

and

Personal Data Processor, Inspera AS,

Incorporated in Norway, company number 998156963, with registered address at Cort Adelers gate 30, 0254 Oslo, Norway (“the Processor”).

1 Background and Purpose

1.1 The parties have already entered into an agreement dated [yyyy-mm-dd] relating to the Controller's use of the Processor's e-assessment platform, Inspera Assessment ("**Agreement**"). On this day the parties have entered the following personal data processing agreement ("**DPA**). The DPA commences as at the date of the parties' execution of the Agreement which is incorporated into and is governed by the terms of the Agreement.

1.2 Any capitalised terms not defined in this DPA shall have the meaning given to it in the Agreement.

The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include personal data ("**Personal Data**"), which means all personal data processed by the Processor on behalf of the Controller, including but not limited to, the personal data as described in clause 2 by on behalf of the Controller, including collection, recording, alignment, storage and disclosure or a combination of such uses. The DPA replaces any other previously entered agreements or agreement terms between the Processor and the Controller regarding handling of Personal Data.

1.3 This DPA shall ensure that the Personal Data covered by the Processor's Processing is managed in accordance with the requirements pursuant to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"), as well as all applicable privacy and data protection laws including the UK Data Protection Act 2018, Norwegian Personal Data Act (Personopplysningsloven) and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (together referred to as "**Data Protection Law**") and that the Personal Data does not become accessible to unauthorised persons.

1.4 This DPA aims to meet the requirements of the GDPR, which require a written DPA regarding the Processor's processing of the Personal Data on behalf of the Controller.

1.5 This DPA shall ensure that personal information relating to the data subjects is not used unlawfully or come into the hands of a third party.

1.6 The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

2 Data Processing Activities to be Performed by the Processor

2.1 The Personal Data transferred will be subject to the following basic activities and used only in connection with these activities: planning, administering, conducting,

monitoring, marking, analysis, marker quality assurance checks and results release activities as well as handling complaints and cheating prevention to allow for assessments of students to be assessed digitally by the Controller.

2.2 Personal Data transferred includes but is not limited to the following categories of data subjects:

- Employees, freelancers and contractors of the Controller
- Students and pupils of the Controller
- End 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.
- Individuals with whom End Users communicate with by email and/or other messaging media.
- Supplier and service providers of the Controller.
- Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.

2.3 The following Personal Data may be stored in the Services and transferred pursuant to this DPA, dependent on the Controller's system configuration:

- End User Full Name (test taker name only if required by the Controller for test taker identification purposes)
- Username
- Password of End Users
- Email address of End Users
- National identification or social security number of End Users (if required by the Controller for test taker identification purposes)
- Student identification number of End Users (if required by the Controller for test taker identification purposes)
- Programme of study, location, cohort, study mode, grade level of End Users (if required by the Controller for reporting)
- Identifying information from 3rd party authentication or authorisation services
- Test submissions including examination questions and answers
- Marking and annotation of test submissions
- Feedback to the test taker
- Internal comments between marker within the system (not published to test taker)
- IP address of the test taker
- Event log of administrative actions defining the test
- Event log of actions during individual test taking
- Process monitoring when using Bring-Your-own-Device (BYOD) to prevent cheating
- Audio and visual recordings of end users, their device screen while taking part in test sessions

- Photo ID of the end user

2.4 The following sensitive or special categories of data are permitted to be collected, transferred and processed by the Controller:

- Biometric data used for identification purposes – in particular facial recognition.

2.5 The Controller grants the Processor the perpetual right to use Statistical Data and nothing in this agreement shall be construed as prohibiting Inspera from using the Statistical Data for internal business and/or operating purposes, provided that the Processor does not share with any third party any Statistical Data, which reveals the identity of the Customer, End Users or Customer's Confidential Information.

2.6 The Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, as may be updated from time to time.

3 The Processor's Obligations

3.1 When processing Personal Data on behalf of the Controller, the Processor shall follow the routines and instructions given by the Controller at any given time.

3.2 The Processor must comply with its obligations under the applicable Data Protection Law and the DPA regarding the documentation and Personal Data to which it has access.

3.3 The Processor must process the Personal Data on documented instructions from the Controller and is not entitled to process Personal Data in any other way other than that which is agreed in writing with the Controller.

3.4 The Processor shall take steps to ensure that any person acting under the authority of the Processor who has access to Personal Data shall only process the Personal Data on the documented instructions of the Controller.

3.5 The Processor shall provide such information and such assistance to the Controller as the Controller may reasonably require, and within the timescales reasonably specified by the Controller, to enable the Controller to comply with its obligations under Data Protection Law and any other applicable law or regulation relating to the processing of Personal Data and to privacy, including assisting the Controller to:

a) comply with its own security obligations;
b) discharge its obligations to respond to requests for exercising data subjects' rights;
c) carry out privacy impact assessments and audit privacy impact assessment compliance; and
d) consult with the applicable supervisory authority following a privacy impact assessment;

3.6 As the volume of these services is not under the Processor's control, nor is it part of the normal services, the Processor's time used to support the Controller in these situations are invoiced at the Processor's standard hourly rates.

3.7 The Processor shall without delay inform the Controller of any communication from any data protection authority, or equivalent authority, that concerns or may be of significance to the processing of the Personal Data. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards any data protection authority or another third party.

3.8 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breaches any Data Protection Law.

3.9 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

3.10 All third-party requests regarding Personal Data or information about the processing activities under the Agreement shall be redirected to the Data Controller, unless such requests cannot legally be redirected to the Data Controller.

3.11 The Processor will make commercially reasonable efforts, to the extent allowed by law and by the terms of the third-party request, to:

a) promptly notify the Controller of the receipt of a third-party request;
b) comply with the Controller's commercially reasonable requests regarding its efforts to oppose a third-party request; and
c) provide the Controller with information or tools required for the Controller to respond to the third-party request (if the Controller is otherwise unable to obtain the information).

3.12 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data. In the event that the Processor receives a request from a data subject in relation to Personal Data, the Processor will refer the data subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a data subject request. In the event that the Processor is legally required to respond to the data subject, the Controller will fully cooperate with the Processor as applicable.

3.13 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller,

unless such notification is not permitted under applicable law or a relevant court order.

3.14 The Processor shall without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("Data Breach").

3.15 The notification shall include:

a) the nature of the Data Breach, including the categories and approximate numbers of data subjects and Personal Data records concerned;
b) the person(s) who destroyed, lost, altered, disclosed, accessed and/or received the Personal Data records concerned (if known);
c) any investigations into such Data Breach;
d) the likely consequences of the Data Breach;
e) any measures taken, or that the Processor recommends, to address the Data Breach, including to mitigate its possible adverse effects; and
f) such other information as the Controller may reasonably require.

3.16 If the Controller or supervisory authority so requests, the Processor shall inform the data subject of the Data Breach in accordance with Data Protection Law. In the case that the Processor does not have the contact information needed to contact the data subject, the Processor will give this information to the Controller, who will contact the data subject.

3.17 In the event of a Data Breach, the Processor shall promptly identify what corrective action the Processor has taken or will take to prevent future Personal Data breaches.

3.18 The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

3.19 The Processor shall keep or cause to be kept such information as is necessary to demonstrate compliance with its obligations in this DPA, including full and accurate records relating to the processing of Personal Data and shall, upon reasonable notice, make available to the Controller or grant to the Controller and its auditors and agents, a right of access to and to take copies of any information or records kept by the Processor pursuant to this DPA.

3.20 The Controller has the right by itself or through a third party to verify that the Processor complies with its obligations under this DPA and any instructions issued by the Controller. The Processor shall, at the expense of the Controller, provide the Controller help and provide the documentation required for this.

3.21 Unless otherwise agreed or pursuant to statutory regulations, the Controller is entitled to access all Personal Data being processed on behalf of the Controller and the systems used for this purpose. The Processor shall provide the necessary and reasonable assistance by contributing to audits, including inspections conducted by

the Data Controller or other auditor authorised by the Data Controller. The working hours spent and reasonable associated costs in respect of audit activities will be borne by the Data Controller.

3.22 The Processor shall reasonably assist the Controller in meeting the Controller's obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Processor.

3.23 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirements including, but not limited to, retention requirements.

4 Confidentiality and Professional Secrecy

4.1 All Processing of Personal Data shall take place in consideration of confidentiality and in compliance with Data Protection Law, which requires the Processor, and its agents, to comply with obligations of confidentiality.

4.2 The Processor is responsible for ensuring that engaged personnel and subcontractors have committed themselves to adhering to their obligations of confidentiality under Data Protection Law. Accordingly, the Processor shall ensure that all persons which the Processor is responsible for and that handle Personal Data pursuant to this DPA sign a confidentiality agreement.

4.3 Unless otherwise provided by compulsory law, the Processor, its employees or sub-processors (meaning any person or entity engaged by the Processor or its Affiliate to process Personal Data in the provision of Services to the Controller) may not disclose any information to a third party without first having obtained the Controller's consent.

5 Use of Sub-Processors

5.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor (meaning any entity that directly or indirectly controls, is controlled by, or is under common control of the Processor) may be used as sub-processors; and (ii) the Processor and its Affiliates respectively may engage sub-processors in connection with the provision of the Services.

5.2 All sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

5.3 The Controller authorises the Processor to use the sub-processors already engaged by the Processor as at the date of the Agreement and the Processor shall make available to the Controller a list of sub-processors available at https://www.inspera.com/legal authorised to process the Personal Data which shall include the identities of sub-processors and their country of location. During the term of this DPA, the Processor shall provide the Controller with prior notification, via email, of any changes to the list of sub-processor(s) before authorising any new or replacement sub-processor(s) to process Personal Data.

5.4 The Controller may object to the use of a new or replacement sub-processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement sub-processor, the Controller may terminate the Agreement with respect to those Services which cannot be provided by the Processor without the use of the new or replacement sub-processor.

5.5 All sub-processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall: (i) prior to the relevant sub-processor carrying out any processing activities in respect of the Personal Data; (ii) appoint each sub-processor under a written contract containing materially the same obligations to those of the Processor in this DPA enforceable by the Processor; and (iii) ensure each such sub-processor complies with all such obligations.

5.6 The Controller agrees that the sub-processors may transfer Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement to countries outside the European Economic Area (EEA). The Processor confirms that such sub-processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses (meaning the EU model clauses for Personal Data transfer from controllers to processors c2010-593 - Decision 2010/87EU) with the Processor; or (iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

5.7 The Controller is able to activate and use integrated end user services provided by third parties. If the Controller uses any third-party service under the Agreement,

a) the third-party service may access or use the Controller's Personal Data; and
b) the Processor will not be responsible for the third-party's use of Personal Data.

6 Security Measures

6.1 The Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6.2 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken

in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

6.3 The technical and organisational measures detailed in the Processor's security statement published at http://www.inspera.com/legal ("Security Statement") shall at all times be adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in the Security Policy and appropriate pursuant to the Processor's obligations in clauses 6.1 and 6.2 above

7 Controller's Obligations

7.1 The Controller represents and warrants that it shall comply with this DPA and its obligations under Data Protection Law.

7.2 The Controller represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Affiliates and sub-processors, to execute their rights or perform their obligations under this DPA.

7.3 All Affiliates (meaning any entity that directly or indirectly controls, is controlled by, or is under common control of the Controller) who use the Services shall comply with the obligations of the Controller set out in this DPA.

7.4 The Controller is responsible for compliance with Data Protection Law, including requirements with regards to the transfer of Personal Data under this DPA and the Agreement.

7.5 The Controller shall implement appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

7.6 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data, the Processor assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. The Processor shall be entitled to charge the Controller for its costs and expenses in providing any such assistance on a time and materials basis.

8 Cooperation

8.1 The parties shall notify each other within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect their contractual duties. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

8.2 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA and Data Protection Law.

9 Amendments and Modifications

9.1 Amendments and modifications to this DPA shall be in writing and signed by authorised representatives of both Parties to be valid.

10 Term

10.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

11 Liability

11.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

11.2 The parties agree that the Processor shall be liable for any breach of this DPA caused by the acts and omissions or negligence of its sub-processors to the same extent the Processor would be liable if performing the services of each sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

11.3 The Controller shall not be entitled to recover more than once in respect of the same loss.

12 Termination

12.1 The Processor shall at the choice of the Controller, upon receipt of a written request received within 50 days of the end of the provision of the Services, delete or return Personal Data to the Controller. The Processor shall in any event anonymise all Personal Data in its systems in a definite/irreversible manner within 180 days of the

effective date of termination of the Agreement or delete, unless applicable law or regulations require storage of the Personal Data after termination.

12.2 Upon request, the Processor shall provide a written notice of which measures taken in relation to the Personal Data in connection with the Processing being terminated.

13 Notifications

13.1 Notifications under this DPA from either party shall be submitted in writing to:

Party	Contact person	Email
The Controller	[Controllers Full Name]	[Controller Email]
The Processor	Lasse Wikmark, DPO	privacy@inspera.com

14 Applicable Law and Disputes

14.1 Subject to any provisions of the Standard Contractual Clauses to the contrary, the Parties' rights and obligations under this DPA shall be governed by laws of England and Wales. Disputes regarding the interpretation or application of this DPA shall be decided in accordance with the laws of England and Wales and the parties hereby submit to the exclusive jurisdiction of the English courts.

Signed for and on behalf of Inspera AS Name and position: [Name, Position] Date: yyyy-mm-dd	Signed for and on behalf of [CONTROLLER] Name and position: [Name, Position] Date: yyyy-mm-dd