Data Processing Agreement

between

PRODUKTIVNORGE AS

as data controller (here referred to as "Principal" or “Data Controller”)

and

Mindmarker

---

as data processor (here referred to as “Contractor“ or “Data Processor”)

This Data Protection Addendum ("Addendum") forms part of any and all agreements between Vendor and Company pursuant to which any Company Personal Data is processed (collectively, the "Principal Agreement") between: (i) MINDMARKER HOLDINGS CORPORATION ("Vendor") acting on its own behalf and as agent for each Vendor Affiliate; and (ii) PRODUKTIVNORGE AS ("Company") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws (including by virtue of any contract relating to such Company Personal Data); and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws (including by virtue of any contract relating to such Company Personal Data);

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;

1.1.5 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 12 below;

For the avoidance of doubt: (a) without limitation to the generality of the foregoing, the parties to this Addendum intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be established under section 12; and (b) where a transfer of Personal Data is of a type authorised by Data Protection Laws in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer.

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.12 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.13 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.14 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. Processing of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2 inform the Company promptly, and in any event before executing on the particular instruction, if Vendor considers that an instruction violates Data Protection Regulations. The Vendor shall then be entitled to suspend the execution of the relevant instructions until the Company confirms or changes them; and

3.1.3 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

Vendor and each Vendor Affiliate shall in relation to the Company Personal Data implement the technical and organisational measures described in Annex 3 to this Addendum.

6. **Subprocessing**

6.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice, Company notifies Vendor in writing of any objections to the proposed

appointment neither Vendor nor any Vendor Affiliate shall appoint (nor disclose any Company Personal Data to) the proposed Subprocessor except with the prior written consent of Company.

6.4 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR; and

6.4.3 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Vendor shall:

7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. **Personal Data Breach**

8.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:

8.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.1.2 communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal Data

10.1 Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within 60 days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

10.2 Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within 30 days of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within 45 days of the Cessation Date.

10.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within 60 days of the Cessation Date.

11. Audit rights

11.1 Subject to sections 11.2 and 11.3, Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate (as "data importer"), hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Company may:

13.4.1 by at least 30 calendar days' written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Company gives notice under section 13.4.1, Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1.

13.6 If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties'

intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

PRODUKTIVNORGE AS	**MINDMARKER HOLDINGS CORPORATION**
By:	By:
Name:	Name: David Froelich
Title:	Title: Chief Executive Officer
Date:	Date: Wed, Nov 4, '20
Signature:	Signature:

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

produktivNorge AS provides training and learning & development services for their customers.

The nature and purpose of the Processing of Company Personal Data

Mindmarker is a provider of a cloud-based Training Reinforcement software solution. The services primarily consist of sending training materials to learners and collecting results of the interaction learners have with that training material. To support that Mindmarker hosts a admin portal where certain privileged users on behalf of Mindmarker customers can create and manage training materials, invite learners and view results of learners for training programs.

The types of Company Personal Data to be Processed

- **Identification information** (First name and last name);
- **Contact information** (Work email address);
- **Technical/Device information** (Ip address, Device brand and model, Operating system and version, Browser brand and version);
- **Training results** (Training completion, Training score)
- **Operational data** (user ID)

The categories of Data Subject to whom the Company Personal Data relates

Employee personal data and training results for initially 1 year. This period can be extended.

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

Standard Contractual Clauses (processors)

Name of the data exporting organisation: **PRODUKTIVNORGE AS**

Address: Balder allé 2, 2060 Gardermoen, Norway

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation

……

(the **data exporter**)

And

Name of the data importing organisation: MINDMARKER HOLDINGS CORPORATION

Address: 275 Grove St, Suite 2-400, Newton, MA 02466, United States of America

Tel.: +1 (617) 213-0776 ; e-mail: legal@mindmarker.com

(the **data importer**)
each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on

the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it

will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):
Position:
Address: Balder allé 2, 2060 Gardermoen, Norway
Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:

Name (written out in full): David Froelich
Position: CEO, Mindmarker, LLC
Address: 275 Grove St, Suite 2-400, Newton, MA 02466 , United States of America

Signature:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

Training employees of produktivNorge AS's clients.

Data importer
The data importer is:

Mindmarker is a provider of a cloud-based Training Reinforcement software solution. The services primarily consist of sending training materials to learners and collecting results of the interaction learners have with that training material. To support that Mindmarker hosts a admin portal where certain privileged users on behalf of Mindmarker customers can create and manage training materials, invite learners and view results of learners for training programs

Data subjects

produktivNorge AS's client's employees

Categories of data
The personal data transferred concern the following categories of data:

- **Identification information** (First name and last name);
- **Contact information** (Work email address);
- **Technical/Device information** (Ip address, Device brand and model, Operating system and version, Browser brand and version);
- **Training results** (Training completion, Training score)
- **Operational data** (user ID)

Processing operations
The personal data transferred will be subject to the following basic processing activities:

The services primarily consist of sending training materials to learners and collecting results of the interaction learners have with that training material.

Mindmarker uses the following sub-processors to support their services.

#	Name of subcontractor	Address of subcontractor	Country	Purpose of commission
1	Amazon Web Services	410 Terry Avenue N, Seattle, WA 98109	USA	Infrastructure services
2	Google Firebase, Analytics, Workspace	1600 Amphitheatre Parkway, Mountain View, CA 94043	USA	Application optimization, web

	(Formerly known as G Suite)			analytics services, team communication
3	Zendesk	San Francisco, California	USA	Customer Service platform
4	Slack	500 Howard Street, San Francisco, CA 94105	USA	Team communication
5	HubSpot	25 First Street, 2nd Floor, Cambridge, Massachusetts 02141	USA	CRM and Marketing tool
6	Atlassian Jira, Bitbucket, Bamboo	341 George Street, Sydney, NSW 2000	Australia	Asset Management and Team Collaboration tool
7	Zeplin	221 Main St #770, San Francisco	USA	UX design collaboration
8	Mailchimp	Atlanta	USA	Product update newsletters
9	Zoom	San Jose, California.	USA	Team communication
10	Webflow	San Francisco, CA	USA	Website building and hosting
11	Datadog	620 8th Avenue, 45th Floor, New York, NY 10018	USA	Monitoring and centralized logging
12	SurveyMonkey	One Curiosity Way, San Mateo, CA 94403	USA	Customer satisfaction surveys

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: David Froelich

Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Information Security Policies

Mindmarker information security policies are written to take account of the specific needs of providing cloud services including:

- Extensive use of virtualization
- The multi-tenanted nature of our services
- Risks from authorized insiders
- Protection of cloud customer data
- The need for effective communication with our customers

All policies are version-controlled, authorized and communicated to all relevant employees and contractors.

Organisation Of Information Security

Roles and responsibilities for the management of the cloud environment are clearly defined as part of contract negotiation so that customer expectations are aligned appropriately with the way that service will be delivered.
In addition, a clear split of responsibilities between Mindmarker and our suppliers, including cloud service providers that supply supporting services, is established and maintained.

Human Resource Security

A comprehensive program of awareness training is delivered on an ongoing basis to all Mindmarker employees to emphasize the need to protect customer cloud data appropriately. We also require our contractors to provide appropriate awareness training to all relevant employees.

Asset Management

An audited procedure is in place for the return and removal of cloud customer assets when appropriate. This procedure is designed to assure the protection of customer data in general and particularly personal data.

Access Control

We provide a comprehensive, user-friendly administration interface to authorized customer administrators that allows them to control access at the service, function and data level. User registration and deregistration and access rights management is achieved via this interface.
Documented procedures for the allocation and management of secret authentication information, such as passwords, ensure that this activity is conducted in a secure way.
The use of utility programs within the customer cloud environment by Mindmarker employees is strictly controlled and audited on a regular basis.
Where we operate a multi-tenanted environment, cloud customer resources are subject to strict segregation from each other, so that no access is permitted to any aspect of another customer's environment, including settings and data.

Virtual machine hardening, including the closing of un-needed ports and protocols, is implemented as standard practice and each virtual machine is configured with the same degree of protection for malware as physical servers.

Cryptography

Transactions between the user (including administrators) and the cloud environment are encrypted using TLS by default. Customer data is encrypted at rest using keys managed by Mindmarker.

Physical And Environmental Security

Mindmarker has procedures in place for the secure disposal and reuse of resources when no longer required by the cloud customer. These procedures will ensure that customer data is not put at risk.

Operations Security

Mindmarker makes customers aware of planned changes that will affect the customer cloud environment or services. This information is published regularly via
email to affected customer administrators and will include the type of change, scheduled date and time and, where appropriate, technical details of the change being made. Further notifications will be issued at the start and end of the change.
The capacity of the overall cloud environment is subject to regular monitoring by Mindmarker engineers to ensure that our capacity obligations can be fulfilled at all times.
Mindmarker ensures data is replicated and backed up in multiple durable encrypted data-stores. The retention period of backups depends on the nature of the data. Data is also replicated across availability zones and infrastructure locations in order to provide fault-tolerance as well as scalability and responsive recovery, when necessary.
In addition, the following policies have been implemented and enforced for data resilience:

- Seven days worth of backups are kept for the production database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary service no less often than daily. All production data is stored on a distributed file storage facility.
- Because we leverage private cloud services for hosting, backup and recovery, Mindmarker does not implement physical infrastructure or physical storage media within its organization. Mindmarker does also not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.
- By default, all backups will be protected through access control restrictions on Mindmarker product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

Activity and transaction logs are recorded in the cloud environment and can be provided upon request to customer administrators. These include details of logins/logouts, data access and amendments/deletions.
The cloud environment is subject to regular vulnerability scanning using industry-standard tools. Critical security patches are applied in accordance with software manufacturers' recommendations.
Operational activities which are deemed critical and in some cases irreversible (such as deletion of virtual servers) are subject to specially controlled procedures which ensure that adequate checking is performed prior to completion. We also recommend that customer put their own procedures in place in these areas.

System Acquisition, Development And Maintenance

Secure development procedures and practices are used within Mindmarker, including separation of development, test and production environments, secure coding techniques, static code analysis and comprehensive security acceptance testing.

Supplier Relationships

In the delivery of certain services, Mindmarker makes use of peer cloud service providers in a supply chain arrangement. These suppliers are subject to regular second party audit to ensure that they have defined objectives for information security and carry out effective risk assessment and treatment practices.
All supplier relationships are covered by contractual terms which meet the requirements of the GDPR.

Information Security Incident Management

Where Mindmarker believes it is appropriate to inform the customer of an information security event (before it has been determined if it should be treated as an incident) we will do this to the nominated customer administrator or deputy. Similarly, the customer may report security events to our support desk where they will be logged and the appropriate action decided. Information about the progress of such events may be obtained from the support desk.
Mindmarker will report information security incidents to the customer where it believes that the customer service or data has or will be affected. We will do this to the nominated customer administrator or deputy as soon as reasonably possible and will share as much information about the impact and investigation of the incident as we believe to be appropriate for its effective and timely resolution. An incident manager will be appointed in each case who will act as the Mindmarker point of contact for the incident, including matters related to the capture and preservation of digital evidence if required.
We prioritise incident management activities to ensure that the timescale requirements of the GDPR for notification of breaches affecting personal data are met.

Information Security Aspects Of Business Continuity Management

Mindmarker plans for and regularly tests, its response to various types of disruptive incident that might affect cloud customer service. The architecture of our cloud services is designed to minimize the likelihood and impact of such an incident and we will make all reasonable efforts to avoid any impact on customer cloud services.

Compliance

The legal jurisdiction of the cloud service provided will depend upon the country in which the contract is made. Where the data of EU citizens is held, Mindmarker will comply with the requirements of the General Data Protection Regulation and/or the EU/USA Privacy Shield. Evidence of our compliance to these requirements is available on request.
Records collected by Mindmarker as part of its provision of the cloud service will be subject to protection in accordance with our information classification scheme and asset handling procedures.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

Measures to protect the processing system

The Contractor has taken the following processing equipment related measures:

#	Measure	Confirmed	Confidentiality	Integrity	Availability	Resilience
3.1	The servers used for processing are located in a server room which is treated as a special protection zone.	Confirmed	x	x		
3.2	There are no water pipes without sufficient overflow protection and no unnecessary fire loads in the server room, where servers are located, with which the data of the Data Controller are processed.	Confirmed			x	
3.3	Maintenance activities by external personnel are only carried out in the server room under supervision.	Confirmed	x	x	x	
3.4	The server room has a mechanism that makes unauthorised access significantly more difficult (e.g. knob on the outside door, puller).	Confirmed	x	x	x	
3.5	Servers on which personal data of the Data Controller are processed and network components used for processing are hardened, insofar as this is possible for functional and maintenance reasons.	Confirmed	x	x	x	
3.6	The server is only operated with personalized	Confirmed	x	x	x	

	administrator accounts.					
3.7	Special protection exists for administrative access to the server (e.g. dedicated access, access only from administration network, two-factor authentication, transport encryption).	Confirmed	x	x	x	
3.8	Administrator accounts ensure higher security than normal user accounts (e.g. with significantly longer passwords, comprehensive password history).	Confirmed	x	x	x	
3.9	Default passwords have been reset for the servers and network components used for processing.	Confirmed	x	x	x	
3.10	If functional accounts are used to administer the server, the passwords of these accounts will be reset as soon as an authorized admin has left the team.	Confirmed	x	x	x	
3.11	Changes carried out on the server are documented and have been tested for safety beforehand by the Data Processor.	Not Confirmed	x	x	x	
3.12	Required security patches are applied promptly.	Confirmed	x	x	x	
3.13	The servers have a secure and sufficiently robust default setting to enable a secure restart of the server	Confirmed				x

	system within the scheduled time.					
3	Number of protection goals achieved	12				

APPENDIX 4 TO THE STANDARD CONTRACTUAL CLAUSES

Measures for proper operation

The Contractor has taken the following measures for the ongoing operation of the agreed activity:

#	Measure	Confirmed	Confidentiality	Integrity	Availability	Resilience
4.1	The personal data of the Data Controller stored by the processor is backed up in accordance with the state of the art.	Confirmed		x	x	x
4.2	Media used for data backup is stored separately from productive servers used to process personal data of the Data Controller.	Confirmed			x	x
4.3	Servers, on which personal data of the Data Controller is stored, have a sufficiently dimensioned uninterruptible power supply.	Confirmed		x	x	
4.4	The personal data of the Data Controller stored by the processor will be deleted after the specified retention period has expired.	Confirmed	x			
4.5	The infrastructure used to complete the job is protected against malware by up-to-date virus scanners.	Confirmed		x		
4.6	The Data Processor has sufficient	Confirmed	x	x	x	

	network segmentation and network segregation.					
4.8	The effectiveness of the measures taken is monitored at least once a year.	Confirmed	x	x	x	x
4.9	If the server system as a whole or components used to operate the server system are to be replaced, it is ensured that no readable data of the Data Controller is left on the data storage media to be disposed of.	Confirmed	x			
4.10	If data storage media are to be disposed of which contain data of the Data Controller, which are stored, transmitted or evaluated by the server system used, these data storage media shall either be physically destroyed or overwritten by means of erasure software in such a way that a reconstruction of the data is no longer possible with justifiable effort.	Confirmed	x			
4.11	The client systems of the persons who access personal data of the Data Controller during the execution of the data processing have a screen protection which, after a sufficiently short period of inactivity, triggers an automatic	Confirmed	x	x	x	

	lock which can only be removed by entering a password.					
4.12	User passwords of the persons used to complete the data processing have a high password complexity with at least eight characters and using upper and lower case letters, numbers and special characters.	Confirmed	x	x	x	
4.13	Access authorizations shall be blocked immediately upon expiry of the validity of the authorizations.	Confirmed	x	x	x	
4.14	Persons who process personal data of the Data Controller will be informed about their obligations.	Confirmed	x	x	x	
4.15	Any security incidents discovered during ongoing operations concerning personal data of the Data Controller shall be reported to the Data Controller without delay.	Confirmed				x
4	Number of protection goals achieved	15				

APPENDIX 5 TO THE STANDARD CONTRACTUAL CLAUSES

Additional security measures to ensure an adequate level of protection of the transferred data

- Data is only hosted in a country where GDPR applies (Ireland).
- Encryption where only the data exporter has the key and which cannot be decrypted by US agencies.
- Anonymization or pseudonymization where only the data exporter can link the data to a natural person.
- MindMarker utilizes AWS WAF for protecting its application from not authorized access and OWASP Top Ten common attacks.