Sub-schedule 1.3 DATA PROCESSING ADDENDUM

Customer is deemed Data Controller and Supplier is deemed Data Processor.

The Data Processing Addendum applies when Clicklearn processes personal data on behalf of the customer.

Background: This data processing agreement, the Clauses, is concluded based on the template included in the following EU legislation:

- Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance)

The Clauses are to be included in the Terms & Conditions between the Parties. The Clauses comes into force and will become effective and binding on the Parties by the signature of the Terms and Conditions.

A few changes have been made in accordance with the user guidance:

- The Annexes in the Clauses have been made more user friendly,
- reference to Regulation (EU) 2018/1725 have been removed as irrelevant, and,
- where mandated, an option in the Clauses have been selected.

Regarding parties outside the EU, The Clauses only apply insofar as the party / the processing activities outside the EU fall under the GDPR and only to the degree as mandated by the GDPR.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

Standard contractual clauses

SECTION I

1. Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with 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 regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

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

(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.

(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.

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 if they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

3. Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, 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.

(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 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

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.

5. 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

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.

7. 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.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 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 organizational 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, unauthorized 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 authorized 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. 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

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

indications of non-compliance. In deciding on a review or an audit, the controller may consider 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 authorization 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 10 calendar 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.

(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 organization by the processor shall only be done on the basis of documented instructions from the controller or in order to fulfil a specific

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

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.

(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.

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 authorized 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, considering 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, considering 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 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organizational 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.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

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 of Regulation (EU) 2016/679, where applicable, considering 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) of 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 of 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);

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

(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.

<div align="center">

SECTION III

FINAL PROVISIONS

</div>

10.   Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, if 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;

    (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.

(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.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

(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.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

List of parties

Controller(s):

Name:

See Terms & Conditions

If relevant, Data Protection Officer (DPO):

N/A

Address:

See Terms & Conditions

Contact person's name, position and contact details:

See Terms & Conditions

Signature and accession date:

(The Clauses comes into force and will become effective and binding on the Parties by the signature of the Terms & Conditions.)

---   --

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

ClickLearn

Processor(s):

Name:

CLICKLEARN ApS, business reg. no. (VAT): 33075731

Address:

Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark (DK)

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

Theis Linnet Aagaard (CFO) | tla@clicklearn.com | +45 21341030

Signature and accession date:

(The Clauses comes into force and will become effective and binding on the Parties by the signature of the Terms & Conditions.)

--   ---

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

Description of the processing

1. Categories of data subjects whose personal data is processed:

> Answer: Employees working for the controller

2. Categories of personal data processed:

> Answer: Personal data under article 6 of the GDPR:
>
> 1. Login information for users: Login-information (e-mail-address, IP-address), full name, role.
>
> 2. End-user utilization: Statistics and certain performance measurement points related to how the service is being used, inter alia End-User identifier, log regarding use of specific content (actions in relation to search, search words, read, view, skipping read and view, reference to recording or documents, assists, user ratings of documents/recordings, external content addressed and used. Further data within the purpose of the End-user utilization may be added.

3. Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

> Answer: No sensitive data are processed.

4. Nature of the processing:

> Answer: The nature of the processing is in relation to providing the service as described in the main agreement to provide user authentication, store, organize, analyse, create statistics, arrange and display data of how the users interact with the content generated by the service.

5. Purpose(s) for which the personal data is processed on behalf of the controller

> Answer: The purpose of the processing is to enable the controller to manage user access to the service and to enable the controller to generate statistics on how the content of the service is utilized to enhance the value of the service.

6. Duration of the processing:

> Answer: The controller decides the duration of the processing. The processor will delete personal data in accordance with communicated retention – and deletion policies insofar as the data controller is not able to technically delete personal data himself.

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

Technical and organizational measures including technical and organizational measures to ensure the security of the data

The level of security shall consider:

That the processing involves a medium volume of personal data which are subject to Article 6 GDPR which is why a 'Medium' level of security should be established.

The data processor has implemented a risk-based approach to IT security and the protection of personal data processed on behalf of the data controller.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that applies and have been agreed with the data controller:

Physical security at the data processor's premises (DK):

Alarm system

Redundant power system

External consultants accessing physical data centre has signed NDA

Key card, access code or similar needed for access to physical data centre

Disaster recovery plan is in place and is regularly (at least yearly) tested

Additional info: There is no physical data centre at data processors' premise. Data hosted in Azure cloud Data centre. We are using on prem server for the internal purpose only. For Disaster recovery we are using the Veaam backup tool.

Physical security at the data processor's premises (IN):

Alarm system

Cooling system

Only access for authorized personnel

External consultants accessing physical data centre has signed NDA

Key card, access code or similar needed for access to physical data centre

Disposing or retiring old hardware is done by procedure and with either secure erase or shredding the data storage

Disaster recovery plan is in place and is regularly (at least yearly) tested

Additional info: There is no physical data centre at data processors' premise. Data hosted in Azure cloud Data centre. Source code is centrally secured in Azure DevOps repo.

Physical security at the data processor's premises (US):

Alarm system

External consultants accessing physical data centre has signed NDA

Key card, access code or similar needed for access to physical data centre

Disaster recovery plan is in place and is regularly (at least yearly) tested

Additional info: There is no physical data centre at data processors' premise. Data hosted in Azure cloud Data centre.

Physical security at the data processor's premises (AU):

Alarm system

External consultants accessing physical data centre has signed NDA

Key card, access code or similar needed for access to physical data centre

Disaster recovery plan is in place and is regularly (at least yearly) tested

Additional info: There is no physical data centre at data processors' premise. Data hosted in Azure cloud Data centre.

Physical security at the data processor's data centre (Azure Cloud Platform):

Alarm system

Cooling system

Redundant power system

Video surveillance

Only access for authorized personnel

External consultants accessing physical data centre has signed NDA

Key card, access code or similar needed for access to physical data centre

Disposing or retiring old hardware is done by procedure and with either secure erase or shredding the data storage

Disaster recovery plan is in place and is regularly (at least yearly) tested

Additional info: Data hosted in Azure cloud Data centre. Microsoft is providing all the security measurements require for data protection and disaster recovery.

Logging (Data Centre: Azure Cloud Platform)

All relevant networks traffic

Server logs (event, security, access, audit etc.)

Database logs (event, security, access, audit etc.)

All access attempts (successful and unsuccessful)

Activities carried out by system admins and others with elevated rights

Security incidents including deactivation of logging, changes to system rights and failed login-attempts

Key card, access code or similar needed for access to physical data centre

The relevant log files are stored and protected against manipulation and technical errors

Additional info: Logging information to access data centre & the servers is handled inside the Azure cloud platform.

Logging (Product: ClickLearn Attain)

Server logs (event, security, access, audit etc.)

Database logs (event, security, access, audit etc.)

Activities carried out by system admins and others with elevated rights

Key card, access code or similar needed for access to physical data centre

The relevant log files are stored and protected against manipulation and technical errors

The log files are continuously monitored

Additional info: Logging information to access ClickLearn Attain are stored in a cloud database system.

Antivirus and firewalls (Data Processor's premise & Azure Data Centre)

All external access to systems and databases where processing of personal data takes place is filtered through a secure firewall with a restrictive protocol.

Use of port and IP-address filtration

Antivirus software on all servers where personal data processing takes place

Antivirus software on all clients where personal data processing takes place

Antivirus continuously updated

Antivirus continuously monitored and automatically trigger event if virus found

Protection against XSS and SQL injections is implemented in all services

The data processors internal networks are only accessible for authorized persons

Encryption

Effective and strong encryption based on a recognized algorithm is used for transmission of personal data though the internet and/or email

A minimum of TLS 1.2 is being used for secure e-mail communication

A minimum of TLS 1.2 is being used, and forced, for secure access to web services (http, API, S-FTP etc.)

Stored sensitive and/or confidential personal data in files is encrypted using a strong algorithm

Stored sensitive and/or confidential personal data in databases is encrypted using a strong algorithm

Stored data is encrypted using an automated generated key

Stored data is encrypted using a AES-256 standard, similar or better

Penetration-test is being done on a regular basis

Vulnerability scan is being done on a regular basis

The results from scans are being used actively to ensure a sufficient level of security and to minimize the impact of hacker-attack, Denial-of-Service attacks etc.

Additional info: We are storing the password as a sensitive personal data apart from general personal data like name and email.

Back up and availability

A change management procedure exists and is being used

Critical patching is done within 4 weeks from evaluating the patch

Security patching is prioritized and done on an asap basis

System monitoring is taking place on all systems where personal data is processed

A guaranteed availability (SLA) exists

A guaranteed availability of more than 98,5%

Back-up is established to ensure that all systems and data, including personal data, can be restored if they are lost or altered.

Back-up resides on alternate location

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

Back-up is public cloud based

Restore can be done within 24 hours

It is logged who requested the restore

It is logged who initiated the restore

Retention period can be defined by the data controller

Additional info: Server security, updates, patch, backup, and availability across the location handled in Azure cloud platform. We are not storing all back in EU region, we are storing the back up in customer's region. i.e., if the customer is located in EU, then backup will be in EU only.

Authorization, access control and security

(Details below provided in the context of data processor's devices and assets.)

Only employees with a work-related demand for personal data are granted access to personal

Data

The assessment of an employee's work-related demands is carried out from a "need-to have" perspective, to ensure compliance with the principle of data minimization

Employees are subject to continuous awareness training in relation to IT security and the security of processing of personal data.

All employees are informed about the management approved information security policy

All potential new employees are subject to screening

When employed, the new employee signs a confidentiality agreement

All new employees are introduced to the information security policy and the procedures for processing of personal data pertaining to the work-related responsibilities of the employee.

The data processor does not operate with shared logins so the data processor will always be able to identify which employee performed a specific activity

Specific procedures are in place to ensure that the access user rights of terminated employees are removed

The data processor has implemented a complex password policy

The data processor has implemented protection of moveable assets (encrypted USB keys etc.)

Laptop computers and other computers processing personal data include protection with commonly recognized encryption

Accessing company data from remote requires VPN or other secure (encrypted) connection

VPN or other secure connection is protected with MFA (Multi Factor Authentication e.g., SMS passcode)

If data is in cloud – MFA is required for admins

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731

If data is in cloud – MFA is required for all users

External consultants are informed of the data processors security guidelines

Risk assessments

In general - risk assessments were performed within the last 12 months

Risk assessment of own data processing on behalf of the data controller

Risk assessments of sub data processors

Risk assessments are approved by the management

If risk assessment shows medium or high-risk appropriate controls or actions of mitigation are applied

Controls

Controls related to authorizations and access are in place

Controls related to authorizations and access are in place

A self-made control 'framework' is in place and actively used

Control responsibilities is assigned appropriate employees

Internal audits are performed regularly

Controls are paired to a risk management approach

Data privacy by design and by default

Data processor is aware of the 'Data protection by design and by default' terminology and guidelines from the European Data Protection Board

Data processor has its own manual, processes, and design guides for ensuring data protection by design and by default

Relevant employees (e.g., architects, designers, and developers) are updated on an on-going basis regarding latest

Relevant employees (e.g., architects, designers, and developers) were updated on latest best-practice within data protection by design and by default within the last 6 months

Implemented default security measures for development is documented and can be shared with data controller

No production data is being used in development environment

No production data is being used in test environment

LIST OF SUB-PROCESSORS

NAME	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft	Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521	**Hosting of services** Data centre use dependent of Customer choice: Western Europe: Amsterdam (EU/EEA location) US: North Central. Canada: Central AUS: Australia East.
ClickLearn India	ClickLearn India Pvt. ltd. Shilp House, Circle, 1002, Sindhu Bhavan Marg, opp. Astral, Bodakdev, Ahmedabad, Gujarat 380058, Indien	**Technical third level support, only.** Will only get access to Customer Data when required on ad hoc basis for third level support.
Clicklearn USA	ClickLearn US, Inc. 200 Central Ave 4th Floor, St. Petersburg, FL 33702, United States of America	**First and second level support,** access to customer data on ad hoc necessity only

Address
Sjæleboderne 2, 1.th,
1122 Copenhagen,
Denmark

Contact
DK: +45 88 77 47 35
US: +1 727-201-5481
engage@clicklearn.com

ClickLearn ApS
www.clicklearn.com
VAT No.: DK33075731