Controller to Processor Agreement

in accordance with Article 28 General Data Protection Regulation[1] (*GDPR*)

This data processing agreement forms an integral part of the Kaspersky end user license agreement ("License agreement") on provision of the Kaspersky Adaptive Online Training Platform ("Product") between:

Kaspersky Lab Switzerland GmbH,
located at address: Bahnhofstrasse 100, 8001 Zürich, Switzerland[2]

- *Processor*-

and

Customer

- *Controller* -

Section 1 Purpose and duration of the agreement

1. Purpose of the agreement

The purpose of the agreement is set out in the written **License agreement.**

2. Duration of the agreement

The duration of the agreement is set out in the written **License agreement.**

Section 2 Scope, manner and purpose of data processing, types of data and categories of data subjects, rights and obligations of the Controller

1. Manner and purpose of data processing

The purpose of the activity of the Processor is set out in the **License agreement.**

2. Types of data

The types of Personal Data are:

- Company ID (if provided)
- First and last name
- Email
- Organizational meta-data (as provided by data-controller), including:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] The definitions of the General Data Protection Regulation apply.

- Department
- Manager
- Employees

- Recorded actions within the system during regular use, including:
  - Content accessed
  - Answers given
  - Time spent
  - Self evaluation scores
  - Completion score
  - Comments and feedback
  - Content created

3. Categories of data subjects

The Categories of Data Subjects are:
(i) Employees of the Data Controller working with the Platform, producing content, learning and/or accessing information about learning.
(ii) Customers of the Data Controller who have purchased access to the Platform via the Data Controller.
(iii) Customers of the Data Controller who have purchased access to the Platform via the Data Processor.

Section 3 Controller's right to instruct

The Processor may process the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Processor shall issue all instructions in text form (e.g. by e-mail). Where instructions are issued orally by way of exception, they shall be appropriately confirmed in text form (e.g. e-mail) by the Controller.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

Section 4 Confidentiality obligation/ obligation to secrecy

The Processor ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Section 5 Processing security / technical and organisational measures pursuant to Article 32 General Data Protection Regulation

The Processor shall take all technical and organisational measures necessary pursuant to Article 32 GDPR. These are set out in detail in **exhibit 1**.

Technical and organisational measures are subject to technological advance and development. For the duration of this agreement, the technical and organisational measures taken shall be continuously adjusted to the requirements of the agreement and shall be advanced further by the Processor in accordance with this agreement and the technological progress. The level of protection must not fall below the technical and organisational measures specified herein and in **exhibit 1**.

The Processor agrees to document major changes to the technical and organisational measures that have a significant impact on the guaranteed safety level in writing as addition to **exhibit 1** and to notify the Controller thereof; such documentation can also be done in electronic form.

Section 6 Engagement of another Processor

The Processor may engage another Processor. Any other Processor engaged at the time the agreement is concluded is listed in exhibit 2 to this agreement. The Processor shall inform the Controller in writing, including in electronic form, of any intended changes concerning the addition or replacement of other Processors. The Controller has the opportunity to object to such changes.

If the Processor engages another Processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act between the Controller and the Processor as referred to in this agreement shall be imposed on that other Processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations.

Section 7 Duty to cooperate / duty to provide assistance

Taking into account the nature of the processing, the Processor assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR (taking into account the data subject’s rights with regard to transparency, right of access, right to rectification, right to erasure (‘right to be forgotten’), right to restriction of processing, notification obligation regarding rectification or erasure of personal data or restriction of processing, right to data portability, right to object, right to automated individual decision-making).

Section 8 Support in fulfilling the Controller´s obligations

The Processor assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Processor (ensuring the security of processing; notification of a personal data breach to the supervisory authority; communication of a personal data breach to the data subject; data protection impact assessment; prior consultation).

Section 9 Deletion and return of personal data

Unless legal or other retention periods apply, Processor shall proceed with the personal data used as follows after completion of the agreement: At the customer's request, the Processor shall hand over this personal data to the Controller in a readable and editable form and delete existing copies, unless the Controller requests the Processor to delete the personal data.

If no request is received from the controller, personal data will be deleted 90 days after the end of the contract with the customer.

Section 10 Proof of obligations and support in inspections

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. He allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

Section 11 Miscellaneous

If the fulfilment of the purpose of the agreement as set out in section 1 of this agreement on the part of Processor is jeopardised as a result of attachment or seizure or of insolvency or settlement proceedings or as a result of other events or measures taken by third parties, the Processor shall notify the Controller immediately. Processor shall immediately notify any and all involved parties that the right to dispose of the data rests solely with the Controller.

In the event of possible discrepancies between this agreement and the **License agreement** the provisions of this agreement shall precede the provisions of the **License agreement**.

The Agreement shall be governed by the law of the EU state in which the data controller is established.

If individual parts of this agreement are invalid, this shall not affect the validity of the remaining parts of this agreement.

Any amendment to this agreement, including its termination and any amendment to this clause, must be made in writing; '*in writing*' shall also include the electronic form.

[**Place**], on [**date**] [**Place**], on [**date**].

_____ _____

- Processor - *- Controller -*

Exhibit 1 Technical and organisational measures pursuant to Article 32 GDPR

Exhibit 2 Other processors

Exhibit 1

Technical and organisational measures pursuant to Article 32 GDPR

Taking into account

- the state of the art,
- the costs of implementation and
- the nature, scope, context and
- purposes of processing as well as
- the risk of varying likelihood and severity for the rights and freedoms of natural persons,

the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Processor meets the following measures:

Organization of Information Security

- There have been appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures
- Personnel with access to Customer Data are subject to confidentiality obligations.
- There has been performed a risk assessment before processing the Personal Data or launching the services.

Asset Management

- Inventory of all assets (in/with which Personal Data are stored) is maintained. Access to inventories of such media is restricted to personnel authorized to have such access.
- Personal Data is classified to help identify it and to allow for access to it to be appropriately restricted
- It is required to obtain special authorization prior to storing Personal Data on portable devices, remotely accessing Personal Data, or processing Personal Data outside of company facilities

Human Resources Security

- Company informs its personnel about relevant security procedures and their respective roles.
- Company also informs its personnel of possible consequences of breaching the security rules and procedures
- Company performs trainings about personal data security

Physical and Environmental Security

- Company limits access to facilities where information systems that process Personal Data are located to identified authorized individuals:
    - 7x24 security service is provided by security guards
    - Perimeter access is controlled by Electronic Access Card System
    - Turnstile is used with proximity card at all entrance points

    - Employees must wear the Company badge
    - Visitors are registered and they must wear visitor badges, Visitors are accompanied during their visit
    - All perimeter access and secure areas are monitored with CCTV, which is monitored by the security guards
- Company maintains records of the incoming and outgoing media, including the kind of media, the authorized sender/recipients, date and time, the number of media.
- A variety of industry standard systems have been implemented to protect against loss of data due to power supply failure or line interference.
- Industry standard processes to delete Personal Data when it is no longer needed have been implemented.

Communications and Operations Management

- Company maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data.
- Copies of Personal Data and data recovery procedures are stored in a different place from where the primary computer equipment processing the Personal Data is located.
- Antimalware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks have been implemented.
- Customer Data, which transmitted over public networks, is encrypted.
- Company logs, access and use of information systems containing Personal Data, registering the access ID, time, authorization granted or denied, and relevant activity.

Access Control

- Company maintains and updates a record of personnel authorized to access systems that contain Customer Data.
- Company identifies those personnel who may grant, alter or cancel authorized access to data and resources.
- Company ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins.
- Technical support personnel are only permitted to have access to Personal Data when needed.
- Company restricts access to Personal Data to only those individuals who require such access to perform their job function.
- Company implements role based access control
- Personnel have been instructed to disable administrative sessions when leaving premises controls or when computers are otherwise left unattended.
- Passwords are stored in a way that makes them unintelligible while they are in force.
- Company uses industry standard practices to identify and authenticate users who attempt to access information systems.
- Company has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered;
- Company password policy defines password complexity requirements;
- All passwords are stored using a one-way hashing algorithm and are never transmitted unencrypted

- Company has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access
- Company internal network channel is protected by implementing firewalls.
- All data transfers between the Company, legal entities and partners and customers are protected with TLS/SSL protocol.

Information Security Incident Management

- Company maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

Vulnerabilities management

- Company's information resources are regularly checked by vulnerability scanners
- Company conducts penetration testing information resources and security audits

Exhibit 2

Other processors

Name and address of another processor	Subject-matter of the subcontracting	Optionally: Date of the conclusion of a contract regarding subcontracting
Amazon Web Services EMEA SARL 5 rue Plaetis L-2338 Luxembourg	Data center provider and cloud provider of virtual computer power and software services. Amazon Web Services EMEA SARL Regions to utilize for end-user data: Germany – AWS Region Frankfurt (EU)	
Area9 Technologies ApS Company reg.no: 34489343 Galionsvej 37, DK 1437 Copenhagen K, Denmark	IT support and server hosting	
Area9 Labs ApS Company reg.no: 25167406 Galionsvej 37, DK 1437 Copenhagen K, Denmark	IT support and server hosting	
Area9 Innovation ApS Company reg.no: 36921897 Galionsvej 37, DK 1437 Copenhagen K, Denmark	IT support and server hosting	
Area9 Lyceum ApS Company reg.no: 39079976 Galionsvej 37, DK 1437 Copenhagen K, Denmark	IT support and server hosting	
Atlassian B.V. c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, CA 94104	IT Support System	
AO Kaspersky Lab, 39A/2 Leningradskoe Shosse, Moscow, 125212, Russian Federation	Providing the initial access to the service, registering of administrators	