**Contratto da titolare del trattamento a responsabile del trattamento**

**In conformità all'articolo 28 del regolamento generale sulla protezione dei dati [1] (*GDPR*)**

Il presente contratto di trattamento dei dati è parte integrante del contratto di licenza con l'utente finale di Kaspersky ("Contratto di licenza") per la fornitura di Kaspersky Adaptive Online Training Platform ("Prodotto") tra:

**Kaspersky Lab Switzerland GmbH,**
**Bahnhofstrasse 100, 8001 Zürich, Svizzera[2]**

*- Responsabile del trattamento -*

e

**cliente**

*- Titolare del trattamento-*

## Sezione 1 Scopo e durata del contratto

### 1. Scopo del contratto

Lo scopo del contratto è indicato nel **contratto di licenza** scritto.

### 2. Durata del contratto

La durata del contratto è indicata nel **contratto di licenza** scritto.

## Sezione 2 Ambito, modalità e finalità del trattamento dei dati, tipi di dati e categorie di interessati, diritti e obblighi del titolare del trattamento

### 1. Metodologia e scopo del trattamento dei dati

Lo scopo dell'attività del responsabile del trattamento è indicato nel **Contratto di licenza.**

### 2. Tipi di dati

I tipi di dati personali sono:

- ID azienda (se fornito)
- Nome e cognome
- E-mail
- Metadati organizzativi (forniti dal responsabile del trattamento dei dati), tra cui:

[1]Regolamento (UE) 2016/679 del Parlamento e del Consiglio europeo del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

[2]Si applicano le definizioni del regolamento generale sulla protezione dei dati.

- Reparto
- Manager
- Dipendenti

- Azioni registrate nel sistema durante l'uso regolare, tra cui:
  - Contenuto consultato
  - Risposte fornite
  - Tempo impiegato
  - Punteggi di autovalutazione
  - Punteggio di completamento
  - Commenti e feedback
  - Contenuto creato

**3. Categorie degli interessati**

Le categorie degli interessati sono:
(i) Dipendenti del titolare del trattamento che lavorano con la piattaforma producendo contenuti, apprendendo e/o accedendo alle informazioni di formazione.
(ii) Clienti del titolare del trattamento che hanno acquistato l'accesso alla piattaforma tramite il titolare del trattamento.
(iii) Clienti del titolare del trattamento che hanno acquistato l'accesso alla piattaforma tramite il responsabile del trattamento.

## Sezione 3 Diritto di istruzione del titolare del trattamento

Il responsabile del trattamento può elaborare i dati personali solo dietro istruzioni documentate fornite dal titolare del trattamento, anche in relazione al trasferimento dei dati personali in un Paese terzo o un'organizzazione internazionale, a meno che non venga richiesto dalla legislazione dell'Unione o degli Stati membri a cui il responsabile del trattamento è soggetto. In tal caso, il responsabile del trattamento deve informare il titolare del trattamento di tale requisito legale prima dell'elaborazione, a meno che la legge non vieti tali informazioni per importanti motivi di interesse pubblico.

Il responsabile del trattamento deve fornire tutte le istruzioni in forma testuale (es. via e-mail). Inviando istruzioni oralmente a titolo di eccezione, esse dovranno essere adeguatamente confermate in forma testuale (es. per e-mail) dal titolare del trattamento.

Il responsabile del trattamento deve informare immediatamente il titolare del trattamento qualora, a suo avviso, un'istruzione violi il GDPR o altre disposizioni sulla protezione dei dati dell'Unione o degli Stati membri.

## Sezione 4 Obbligo di riservatezza/segretezza

Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali abbiano sottoscritto l'impegno a garantire la riservatezza o l'obbligo legale di riservatezza.

## Sezione 5 Misure di sicurezza/tecniche e organizzative per l'elaborazione ai sensi dell'articolo 32 del regolamento generale sulla protezione dei dati

Il responsabile del trattamento intraprenderà tutte le misure tecniche e organizzative necessarie ai sensi dell'articolo 32 del GDPR. Questi elementi vengono descritti in dettaglio nell'**allegato 1**.

Le misure tecniche e organizzative sono soggette al progresso e allo sviluppo tecnico. Per la durata del presente contratto, le misure tecniche e organizzative adottate devono essere costantemente adeguate ai requisiti del contratto e ulteriormente sviluppate dal responsabile del trattamento in conformità al presente contratto e all'evoluzione tecnologica. Il livello di protezione non deve essere inferiore alle misure tecniche e organizzative specificate nel presente documento e nell'**allegato 1**.

Il responsabile del trattamento si impegna a documentare per iscritto le principali modifiche apportate alle misure tecniche e organizzative con impatto significativo sul livello di sicurezza garantito in aggiunta all'**allegato 1** e a informare il titolare del trattamento. Tale documentazione può essere anche di forma elettronica.

## Sezione 6 Coinvolgimento di un altro responsabile del trattamento

Il responsabile del trattamento può contattare un altro responsabile del trattamento. Qualsiasi altro responsabile del trattamento incaricato al momento della conclusione del contratto verrà elencato nell'allegato 2 del presente contratto. Il responsabile del trattamento deve informare il titolare del trattamento per iscritto, anche in formato elettronico, delle eventuali modifiche previste relative all'aggiunta o sostituzione di altri responsabili del trattamento. Il titolare del trattamento potrà opporsi a tali modifiche.

Se il responsabile del trattamento si impegna con un altro responsabile del trattamento per lo svolgimento di attività di trattamento specifiche per conto del titolare del trattamento, gli stessi obblighi di protezione dei dati definiti nel contratto o in altri atti giuridici tra il titolare del trattamento e il responsabile del trattamento di cui al presente contratto verranno imposti a tale altro responsabile del trattamento mediante un contratto o altro atto giuridico ai sensi del diritto dell'Unione o degli Stati membri, in particolare fornendo garanzie sufficienti per mettere in atto adeguate misure tecniche e organizzative in modo che il trattamento soddisfi i requisiti del GDPR. Se l'altro responsabile del trattamento non dovesse adempiere ai propri obblighi in materia di protezione dei dati, il responsabile del trattamento iniziale resterà pienamente responsabile nei confronti del titolare del trattamento per l'adempimento degli obblighi dell'altro responsabile del trattamento.

## Sezione 7 Dovere di collaborazione/offerta di fornire assistenza

Alla luce della natura del trattamento, il responsabile del trattamento assisterà il titolare del trattamento attraverso adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per l'adempimento dell'obbligo del responsabile del trattamento di risposta alle richieste di esercizio dei diritti dell'interessato, di cui al capitolo III del GDPR (tenendo conto dei diritti dell'interessato in materia di trasparenza, diritto di accesso, diritto di rettifica, diritto alla cancellazione o "diritto all'oblio", diritto alla limitazione del trattamento, obbligo di notifica in materia di rettifica o cancellazione dei dati personali o limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto al processo decisionale individuale automatizzato).

**Sezione 8 Supporto dell'adempimento degli obblighi del titolare del trattamento**

Il responsabile del trattamento assisterà il titolare del trattamento nel rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni disponibili per il responsabile del trattamento (garanzia della sicurezza del trattamento, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione dell'impatto sulla protezione dei dati, consultazione preventiva).

**Sezione 9 Cancellazione e restituzione dei dati personali**

A meno che non vengano applicati periodi di conservazione legali o di altro tipo, il responsabile del trattamento utilizzerà i dati personali come segue dopo il completamento del contratto: su richiesta del cliente, il responsabile del trattamento consegnerà questi dati personali al titolare del trattamento in forma leggibile e modificabile ed eliminerà le copie esistenti, a meno che il titolare del trattamento non richieda al responsabile del trattamento di eliminare i dati personali.

Se non viene ricevuta alcuna richiesta dal responsabile del trattamento, i dati personali verranno eliminati 90 giorni dalla scadenza del contratto con il cliente.

**Sezione 10 Prova degli obblighi e supporto nelle ispezioni**

Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare la conformità agli obblighi previsti dall'articolo 28 del GDPR. Questi permetterà e agevolerà le verifiche, comprese le ispezioni, condotte dal titolare del trattamento o da un altro revisore da esso incaricato.

**Sezione 11 Varie**

Se l'adempimento della finalità del contratto, come stabilito nella sezione 1 del presente contratto, da parte del responsabile del trattamento venisse compromesso a seguito di un'ordinanza di sequestro, confisca o procedure concorsuali o di insolvenza o altri eventi o misure adottate da terze parti, il responsabile del trattamento deve informare immediatamente il titolare del trattamento. Il responsabile del trattamento comunicherà immediatamente a tutte le parti interessate la spettanza esclusiva del diritto di eliminazione dei dati al titolare del trattamento.

In caso di eventuali discrepanze tra il presente contratto e il **Contratto di licenza**, le disposizioni presenti nel presente contratto avranno precedenza su quelle presenti nel **Contratto di licenza**.

Il contratto è regolato dalla legge dello Stato dell'UE in cui viene definito il responsabile del trattamento.

Se singole parti del presente contratto non divenissero più valide, tale scenario non pregiudicherà la validità delle restanti parti del presente contratto.

Qualsiasi modifica apportata al presente contratto, inclusa la risoluzione e qualsiasi modifica alla presente clausola, deve essere effettuata per iscritto, dove "*per iscritto*" comprende anche un formato elettronico.

[**Luogo**], il [**Data**] [**Luogo**], il [**Data**].

_____ _____

*- Responsabile del trattamento -* *- Titolare del trattamento-*

**Allegato 1 Misure tecniche e organizzative ai sensi dell'articolo 32 GDPR**

**Allegato 2 Altri responsabili del trattamento**

**Allegato 1**

**Misure tecniche e organizzative ai sensi dell'articolo 32 GDPR**

Tenendo in considerazione

- l'avanguardia tecnologica,
- i costi di attuazione e
- la natura, portata, il contesto e
- le finalità del trattamento e
- il rischio di variazione della probabilità e gravità per i diritti e le libertà delle persone fisiche,

il responsabile del trattamento deve mettere in atto adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.

Nel valutare il livello adeguato di sicurezza occorre tenere conto dei rischi presentati dal trattamento, in particolare da elementi come distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso a dati personali trasmessi, archiviati o trattati in altro modo.

Il responsabile del trattamento deve mettere in atto le seguenti misure:

**Organizzazione della sicurezza delle informazioni**

- Sono stati nominati uno o più responsabili della sicurezza incaricati di coordinare e monitorare le norme e le procedure di sicurezza
- Il personale con accesso ai dati personali del cliente è soggetto a rispettare gli obblighi di riservatezza.
- È stata eseguita una valutazione dei rischi prima di elaborare i dati personali o rendere disponibili i servizi.

**Gestione delle risorse**

- Viene tenuto un inventario di tutte le risorse (in cui o con cui vengono archiviati i dati personali). L'accesso agli inventari di tali elementi multimediali è limitato al personale autorizzato.
- I dati personali vengono classificati in modo da facilitarne l'identificazione e consentire un'adeguata limitazione dell'accesso agli stessi
- È necessario ottenere un'autorizzazione speciale prima di archiviare i dati personali su dispositivi portatili, accedervi in remoto o elaborarli fuori dalle strutture dell'azienda

**Sicurezza delle risorse umane**

- La società mette al corrente i propri dipendenti delle procedure di sicurezza pertinenti e dei loro rispettivi ruoli.
- Inoltre, la società informa il personale delle possibili conseguenze delle violazioni delle norme e procedure di sicurezza
- La società offre un'adeguata formazione sulla sicurezza dei dati personali

**Sicurezza fisica e ambientale**

- La società limita a determinati soggetti autorizzati l'accesso alle strutture in cui sono ubicati i sistemi informativi utilizzati per il trattamento dei dati personali:

    - Gli addetti alla sicurezza forniscono un servizio di protezione attivo 24 ore al giorno e 7 giorni su 7
    - Il perimetro di accesso viene controllato tramite un sistema di accesso elettronico con ID
    - Tutti i punti di entrata prevedono l'utilizzo di tornello e scheda di prossimità
    - I dipendenti devono indossare il badge aziendale
    - I visitatori vengono registrati, devono indossare un badge ed essere accompagnati nel corso della visita
    - L'accesso al perimetro e alle aree sicure viene monitorato tramite TV a circuito chiuso controllate dagli addetti alla sicurezza
- La società conserva registri degli elementi multimediali in entrata e in uscita, che comprendono tipologia di tali elementi, mittenti/destinatari autorizzati, data e ora e numero di elementi.
- Sono stati implementati diversi sistemi standard di settore per la protezione nei confronti delle perdite di dati dovute a interruzione dell'alimentazione o interferenze sulla linea.
- Quando i dati personali non saranno più necessari, verranno adottate procedure standard di settore per eliminarli.

**Gestione delle comunicazioni e operazioni**

- La società mantiene aggiornati i documenti di sicurezza descrivendone le relative misure, le procedure pertinenti e le responsabilità del personale dotato di accesso ai dati personali.
- Le copie dei dati personali e le procedure di recupero dei dati vengono archiviate in un'ubicazione diversa da quella delle apparecchiature informatiche principali per il trattamento dei dati personali.
- Vengono utilizzati controlli anti-malware per impedire che software dannosi ottengano l'accesso non autorizzato ai dati personali, compresi i software dannosi provenienti dalle reti pubbliche.
- I dati personali trasmessi su reti pubbliche verranno crittografati.
- La società registra l'accesso e l'utilizzo dei sistemi informatici che contengono i dati personali, annotando ID di accesso, orario, concessione o rifiuto dell'autorizzazione e attività pertinenti.

**Controllo degli accessi**

- La società gestisce e aggiorna un registro del personale autorizzato all'accesso ai sistemi che contengono i dati personali.
- La società accerta l'identità del personale in grado di concedere, alterare o annullare l'accesso autorizzato ai dati e alle risorse.
- Qualora più soggetti abbiano accesso ai sistemi contenenti i dati personali, la società fa in modo che le persone utilizzino dati di accesso/identificativi diversi.
- Al personale di assistenza tecnica è consentito l'accesso ai dati personali solo se necessario.
- La società limita l'accesso ai dati personali solo ai soggetti che richiedono tale accesso per lo svolgimento del proprio lavoro.
- La società implementa il controllo degli accessi in base al ruolo
- Il personale ha ricevuto istruzioni per disattivare le sessioni amministrative una volta abbandonato il controllo delle strutture o quando i computer vengono lasciati incustoditi.
- Le password vengono memorizzate in modo da renderle non decifrabili durante il periodo di validità.

- La società utilizza pratiche standard di settore per identificare e autenticare gli utenti che tentano di accedere ai sistemi informatici.
- La società ha adottato un'informativa sulle password che ne proibisce la condivisione, disciplina le modalità di intervento in caso di divulgazione, chiede di cambiare regolarmente le password e di modificare quelle predefinite
- L'informativa sulle password della società definisce i requisiti di complessità delle stesse
- Tutte le password vengono archiviate utilizzando un algoritmo di hash unidirezionale e non vengono mai trasmesse in forma non crittografata
- La società dispone di controlli atti a impedire ai soggetti l'attribuzione illecita dei diritti di accesso per consultare i dati personali per i quali non dispongono dell'autorizzazione
- Il canale di rete interno della società è protetto tramite l'implementazione di firewall.
- Tutti i trasferimenti di dati tra società, soggetti giuridici, partner e clienti sono protetti tramite protocollo TLS/SSL.

**Gestione degli incidenti di sicurezza informatica**

- La società registra le violazioni della sicurezza unitamente a una descrizione, al periodo di tempo, alle conseguenze, al nome del segnalatore e al destinatario della segnalazione, nonché alla procedura per il recupero dei dati.

**Gestione delle vulnerabilità**

- La risorse informatiche della società vengono verificate regolarmente dagli addetti all'identificazione delle vulnerabilità
- La società esegue test di penetrazione per verificare le risorse informatiche e controlli della sicurezza

**Allegato 2**

**Altri titolari del trattamento**

| Nome e indirizzo di un altro titolare del trattamento | Oggetto del subappalto | Facoltativamente: data della conclusione di un contratto relativo al subappalto |
|---|---|---|
| Amazon Web Services EMEA SARL<br>5 rue Plaetis<br>L-2338 Lussemburgo | Provider di data center e cloud di servizi IT e software per computer virtuali.<br><br>Regioni di Amazon Web Services EMEA SARL da utilizzare per i dati dell'utente finale: Germania, Regione AWS Francoforte (UE) | |
| Area9 Technologies ApS<br>N° registro società: 34489343<br>Galionsvej 37, DK 1437 Copenhagen K, Danimarca | Supporto IT e hosting server | |
| Area9 Labs ApS<br>N° registro società: 25167406<br>Galionsvej 37, DK 1437 Copenhagen K, Danimarca | Supporto IT e hosting server | |
| Area9 Innovation ApS<br>N. registro società: 36921897<br>Galionsvej 37, DK 1437 Copenhagen K, Danimarca | Supporto IT e hosting server | |
| Area9 Lyceum ApS<br>N. registro società: 39079976<br>Galionsvej 37, DK 1437 Copenhagen K, Danimarca | Supporto IT e hosting server | |
| Atlassian B.V.<br>c/o Atlassian, Inc.<br>350 Bush Street, Floor 13<br>San Francisco, CA 94104, USA | Sistema di supporto IT | |
| AO Kaspersky Lab, 39A/2 Leningradskoe Shosse, Moscow, 125212, Federazione russa | Offerta dell'accesso iniziale al servizio, registrazione degli amministratori | |