Contrat entre le contrôleur et le processeur

conformément à l'article 28 du règlement général sur la protection des données[1] (*RGPD*)

Cet accord de traitement des données fait partie intégrante du contrat de licence d'utilisateur final de Kaspersky (« accord de licence ») relatif à la fourniture de la plate-forme Kaspersky Adaptive Online Training Platform (« produit ») conclu entre :

Kaspersky Lab Switzerland GmbH,
situé à l'adresse : Bahnhofstrasse 100, 8001 Zürich, Suisse[2]

- Processeur -

et

Client

- Contrôleur -

Section 1 Objet et durée du contrat

1. Objet du contrat

Le but du contrat est défini dans le **contrat de licence** écrit.

2. Durée du contrat

La durée du contrat est définie dans le **contrat de licence** écrit.

Section 2 Portée, méthode et but du traitement des données, types de données et catégories de personnes concernées, droits et obligations du Contrôleur

1. Méthode et objet des activités de traitement des données

Le but de l'activité du Processeur est défini dans le **Contrat de licence.**

2. Types de données

Les types de données personnelles sont :

- Identifiant de la société (si fourni)
- Prénom et nom
- E-mail
- Métadonnées de l'organisation (fournies par le contrôleur de données), incluant :

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[2] Les définitions du Règlement général sur la protection des données s'appliquent.

- Département
- Manager
- Employés

- Actions enregistrées dans le système lors de son utilisation régulière, y compris :
  - Contenu consulté
  - Réponses données
  - Temps dépassé
  - Notes d'auto-évaluation
  - Note finale
  - Commentaires et réactions
  - Contenu créé

3. Catégorie de personnes concernées

Les catégories de personnes concernées sont :
(i) Les employés du Contrôleur de données qui travaillent avec la plate-forme, qui produisent des contenus, qui apprennent et/ou qui accèdent à des informations au sujet de l'apprentissage.
(ii) Les clients du Contrôleur de données qui ont acheté un accès à la plate-forme par le biais du contrôleur de données.
(iii) Les clients du contrôleur de données qui ont acheté un accès à la plate-forme par le biais du Processeur de données.

Section 3 Droit d'instruction du Contrôleur

Le Processeur peut traiter les données personnelles uniquement sur les instructions documentées du Contrôleur, notamment en ce qui concerne les transferts de données personnelles vers un pays tiers ou une organisation internationale, à moins qu'il ne soit tenu de le faire par le droit de l'Union ou d'un État membre auquel le Processeur est assujetti. Dans ce cas, le Processeur informera le Contrôleur de cette exigence juridique avant le traitement, à moins que la loi n'interdise ces informations pour des raisons importantes d'intérêt public.

Le Processeur fournira toutes les instructions sous forme de texte (p. ex., par courrier électronique). Si des instructions sont transmises oralement à titre exceptionnel, elles devront être confirmées de manière appropriée sous forme de texte (p. ex., par courrier électronique) par le Contrôleur.

Le Processeur devra informer immédiatement le Contrôleur si, à son avis, une instruction enfreint les dispositions du RGPD ou d'autres dispositions de l'Union ou des États membres en matière de protection des données.

Section 4 Obligation de confidentialité/obligation de discrétion

Le Processeur s'assure que les personnes autorisées à traiter les données personnelles se sont engagées à respecter la confidentialité ou ont une obligation statutaire appropriée de confidentialité.

Section 5 Sécurité du traitement/mesures techniques et organisationnelles en vertu de l'article 32 du Règlement général sur la protection des données

Le Processeur devra prendre toutes les mesures techniques et organisationnelles nécessaires en vertu de l'article 32 du RGPD. Celles-ci sont exposées en détail dans la **pièce 1**.

Les mesures techniques et organisationnelles dépendent des progrès et développements technologiques. Pendant toute la durée du présent contrat, les mesures techniques et organisationnelles prises seront adaptées en permanence aux exigences du contrat et le Processeur les fera évoluer conformément à ce contrat et aux progrès technologiques. Le niveau de protection ne doit pas descendre en dessous des mesures techniques et organisationnelles prévues aux présentes et dans la **pièce 1**.

Le Processeur accepte de documenter par écrit les changements majeurs apportés aux mesures techniques et organisationnelles ayant un impact significatif sur le niveau de sécurité garanti en tant qu'annexe au **schéma 1** et d'en informer le Contrôleur ; cette documentation peut également être effectuée sous forme électronique.

Section 6 Engagement d'un autre Processeur

Le Processeur peut engager un autre Processeur. Tout autre Processeur engagé au moment de la signature du contrat est répertorié dans la pièce 2 jointe au présent contrat. Le Processeur informera le Contrôleur par écrit, y compris sous forme électronique, de tout projet de modification concernant l'ajout ou le remplacement d'autres Processeurs. Le Contrôleur a la possibilité de s'opposer à ces modifications.

Si le Processeur engage un autre Processeur pour mener à bien des activités de traitement spécifiques pour le compte du Contrôleur, les mêmes obligations de protection des données figurant dans le présent contrat ou dans tout autre acte juridique entre le Contrôleur et le Processeur visés par le présent contrat seront imposées à ce tiers au moyen d'un contrat ou d'un autre acte juridique en vertu du droit de la loi de l'Union ou de l'État membre, et fourniront notamment suffisamment de garanties pour mettre en œuvre les mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences du RGPD. En cas de manquement de cet autre Processeur à ses obligations en matière de protection des données, le Processeur initial reste entièrement responsable envers le Contrôleur de l'exécution des obligations de cet autre Processeur.

Section 7 Devoir de coopération/devoir d'assistance

Compte tenu de la nature du traitement, le Processeur aide le Contrôleur au moyen de mesures techniques et organisationnelles appropriées, dans la mesure où cela est possible, pour remplir l'obligation du contrôleur à répondre aux demandes d'exercice des droits de la personne concernée prévues au chapitre III du RGPD (en tenant compte des droits de la personne concernée en matière de transparence, de droit d'accès, de droit de rectification, de droit à l'effacement [« droit à l'oubli »], de droit à la restriction du traitement, de l'obligation de notification concernant la rectification ou l'effacement des données personnelles ou la restriction du traitement, du droit à la portabilité des données, du droit d'objection, du droit à la prise de décision individuelle automatisée).

Section 8 Soutien pour remplir les obligations du Contrôleur

Le Processeur aide le Contrôleur à assurer le respect de ses obligations des obligations en vertu des articles 32 à 36, en tenant compte de la nature du traitement et des informations à la disposition du Processeur (assurer la sécurité du traitement, la notification de toute violation des données personnelles à l'autorité de surveillance, la communication de toute violation des données personnelles à la personne concernée, l'évaluation de l'impact de la protection des données, la consultation préalable).

Section 9 Suppression et restitution des données personnelles

À moins que des périodes de conservation légales ou autres s'appliquent, le Processeur doit procéder comme suit avec les données personnelles utilisées après la fin du contrat : à la demande du client, le Processeur devra remettre ces données personnelles au Contrôleur sous une forme lisible et modifiable et supprimera les copies existantes, à moins que le Contrôleur ne demande au processeur de supprimer les données personnelles.

Si aucune demande n'est reçue de la part du contrôleur, les données personnelles seront supprimées 90 jours après la fin du contrat avec le client.

Section 10 Preuve des obligations et soutien lors des inspections

Le Processeur met à la disposition du Contrôleur toutes les informations nécessaires pour démontrer sa conformité vis-à-vis des obligations prévues à l'article 28 du RGPD. Il autorise et contribue aux audits, et notamment aux inspections, menés par le Contrôleur ou tout autre auditeur mandaté par le Contrôleur.

Section 11 Divers

Si la réalisation par le Processeur de l'objet du contrat stipulé à l'article 1 du présent contrat est compromise en raison d'une saisie-arrêt, d'une saisie ou d'une procédure d'insolvabilité ou de règlement ou à la suite d'autres événements ou de mesures prises par des tierces parties, le Processeur devra en aviser le Contrôleur immédiatement. Le Processeur informera immédiatement toutes les parties concernées que le droit de disposer des données appartient uniquement au contrôleur.

En cas de divergence possible entre le présent contrat et le **contrat de licence**, les dispositions du présent contrat précéderont les dispositions du **contrat de licence**.

Le contrat sera régi par le droit de l'État de l'Union européenne où le contrôleur de données est établi.

Si différentes parties du présent contrat sont invalides, cela n'affectera pas la validité des autres parties du contrat.

Toute modification apportée au présent contrat, y compris sa résiliation et toute modification de la présente clause, doit être effectuée par écrit, « *par écrit* » incluant également un format électronique.

[**Lieu**], le [**date**] [**Lieu**], le [**date**].

_____ _____

- Processeur - *- Contrôleur -*

Pièce 1 Mesures techniques et organisationnelles en vertu de l'article 32 du RGPD

Pièce 2 Autres processeurs

Pièce 1

Mesures techniques et organisationnelles en vertu de l'article 32 du RGPD

Compte tenu de

- la technologie,
- des coûts de mise en œuvre et
- de la nature, la portée, le contexte et
- des objectifs du traitement de données ainsi que
- du risque (d'une probabilité et d'une gravité variables) d'atteinte aux droits et libertés des personnes physiques,

le Processeur mettra en œuvre des mesures techniques et organisationnelles appropriées pour garantir le niveau de sécurité adapté au risque.

Pour évaluer le niveau de sécurité approprié, il convient notamment de tenir compte des risques que présente le traitement, en particulier de la destruction accidentelle ou illicite, la perte, la modification, la divulgation non autorisée ou l'accès aux données personnelles transmises, stockées ou traitées d'une autre façon.

Le Processeur répond aux mesures suivantes :

Organisation de la sécurité des informations

- Un ou plusieurs agents de sécurité ont été nommés responsables de la coordination et du contrôle des règles et procédures de sécurité
- Le personnel ayant accès aux données du client est soumis à des obligations de confidentialité.
- Une évaluation des risques a été réalisée avant le traitement des données personnelles ou le lancement des services.

Gestion des actifs

- L'inventaire de tous les actifs (dans ou avec lesquels les données personnelles sont conservées) est tenu à jour. L'accès aux inventaires de ces supports est limité au personnel autorisé à y accéder.
- Les données personnelles sont classées pour aider à leur identification et permettre de restreindre leur accès de manière appropriée
- Il est nécessaire d'obtenir une autorisation spéciale avant de stocker des données personnelles sur des appareils portables, d'accéder à distance à des données personnelles ou de traiter des données personnelles en dehors des installations de la société

Sécurité des ressources humaines

- La société informe les membres de son personnel des procédures de sécurité pertinentes et de leur rôle respectif.
- La société informe également son personnel des conséquences possibles d'une violation des règles et procédures de sécurité
- La société dispense des formations sur la sécurité des données personnelles

Sécurité physique et environnementale

- La société limite l'accès aux installations où se trouvent des systèmes d'information qui traitent les données personnelles à des personnes autorisées identifiées :
    - Un service de sécurité disponible 7 jours sur 7, 24 h/24, est assuré par des agents de sécurité
    - Le périmètre d'accès est contrôlé par un système de cartes d'accès électronique
    - Des tourniquets sont utilisés avec des cartes de proximité à tous les points d'entrée
    - Les employés doivent porter un badge de la société
    - Les visiteurs sont enregistrés et doivent porter des badges visiteurs ; les visiteurs sont accompagnés pendant leur visite
    - Tous les accès au périmètre et toutes les zones sécurisées sont surveillés par un système de vidéosurveillance, lui-même surveillé par les agents de sécurité
- La société tient à jour les dossiers des supports entrants et sortants, y compris le type de support, l'expéditeur/les destinataires autorisés, la date et l'heure, le nombre de supports.
- Divers systèmes standard de l'industrie ont été mis en œuvre pour assurer une protection contre la perte de données due à une défaillance d'alimentation électrique ou à des interférences de ligne.
- Des processus standard de l'industrie ont été mis en œuvre pour supprimer les données personnelles lorsqu'elles ne sont plus nécessaires.

Gestion des communications et des opérations

- La société assure la sécurité des documents décrivant ses mesures de sécurité et les procédures pertinentes, ainsi que les responsabilités des membres de son personnel qui ont accès aux données personnelles.
- Des copies des données personnelles et des procédures de récupération des données sont stockées dans un endroit distinct de celui dans lequel se trouve l'équipement informatique principal de traitement des données personnelles.
- Des contrôles contre les logiciels malveillants visant à éviter que des logiciels malveillants n'accèdent à des données personnelles sans y être autorisés, et notamment des logiciels malveillants provenant de réseaux publics, ont été mis en œuvre.
- Les données personnelles qui sont transmises sur des réseaux publics sont chiffrées.
- La société enregistre l'accès et l'utilisation des systèmes d'information contenant des données personnelles, en enregistrant l'identifiant d'accès, l'heure, l'autorisation accordée ou refusée et l'activité afférente.

Contrôle d'accès

- La société conserve et tient à jour un registre des personnes autorisées à accéder aux systèmes qui contiennent des données personnelles.
- La société identifie les membres du personnel qui peuvent accorder, modifier ou annuler l'accès autorisé aux données et ressources.
- La société garantit que lorsque plus d'une personne a accès à des systèmes contenant des données de clients, les individus ont des identifiants/connexions distincts.
- Le personnel en charge de l'assistance technique est uniquement autorisé à avoir accès aux données personnelles lorsque cela s'avère nécessaire.
- La société restreint l'accès aux données personnelles aux seules personnes qui ont besoin de cet accès pour exécuter leurs fonctions.
- La société met en œuvre un contrôle des accès en fonction des rôles

- Les membres du personnel ont été invités à désactiver les sessions d'administration lorsqu'ils quittent les locaux de contrôle ou lorsque les ordinateurs sont autrement laissés sans surveillance.
- Les mots de passe sont stockés de manière à être illisibles lorsqu'ils sont en vigueur.
- La société utilise des pratiques standard de l'industrie pour identifier et authentifier les utilisateurs qui tentent d'accéder à des systèmes d'information.
- La société a créé une stratégie de mot de passe qui interdit le partage des mots de passe, détermine les mesures à prendre lorsqu'un mot de passe est divulgué, requiert un changement régulier des mots de passe et une modification des mots de passe par défaut ;
- La stratégie de la société en matière de mot de passe définit les exigences de complexité des mots de passe ;
- Tous les mots de passe sont stockés à l'aide d'un algorithme de hachage unidirectionnel et ne sont jamais transmis sous forme non chiffrée
- La société dispose de contrôles pour éviter que des personnes n'assument des droits d'accès qui ne leur ont pas été assignés pour obtenir l'accès à des données de clients auxquelles elles ne sont pas autorisées à accéder
- Le canal du réseau interne de la société est protégé par la mise en place de pare-feu.
- Tous les transferts de données entre la société, des personnes morales, les partenaires et les clients sont protégés au moyen du protocole TLS/SSL.

Gestion des incidents de sécurité des informations

- La société conserve une trace des violations de sécurité avec une description de la violation, sa période, ses conséquences, le nom de la personne qui l'a signalée, celle à qui on l'a signalée, et la procédure pour la récupération des données.

Gestion des vulnérabilités

- Les ressources d'information de la société sont régulièrement contrôlées par les scanners de vulnérabilité
- La société effectue des tests de pénétration des ressources d'information et des audits de sécurité

Tableau 2

Autres processeurs

Nom et adresse de l'autre processeur	Objet de la sous-traitance	Facultatif : Date de la conclusion d'un contrat concernant la sous-traitance
Amazon Web Services EMEA SARL 5 rue Plaetis L-2338 Luxembourg	Fournisseur de centre de données et fournisseur en nuage de puissance informatique virtuelle et de services logiciels. Amazon Web Services EMEA SARL Régions à utiliser pour les données concernant les utilisateurs finaux : Allemagne – AWS Région de Francfort (UE)	
Area9 Technologies ApS Société n° : 34489343 Galionsvej 37, DK 1437 Copenhague K, Danemark	Assistance informatique et hébergement de serveur	
Area9 Labs ApS Société n° : 25167406 Galionsvej 37, DK 1437 Copenhague K, Danemark	Assistance informatique et hébergement de serveur	
Area9 Innovation ApS Société n° : 36921897 Galionsvej 37, DK 1437 Copenhague K, Danemark	Assistance informatique et hébergement de serveur	
Area9 Lyceum ApS Société n° : 39079976 Galionsvej 37, DK 1437 Copenhague K, Danemark	Assistance informatique et hébergement de serveur	
Atlassian B.V. c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, CA 94104	Assistance informatique des systèmes	
AO Kaspersky Lab, 39A/2 Leningradskoe Shosse, Moscou, 125212, Fédération de Russie	Provision de l'accès initial au service, enregistrement des administrateurs	