Contrato entre el responsable de los datos y el encargado de su tratamiento

de conformidad con el Artículo 28 del Reglamento General de Protección de Datos[1] (*RGPD*)

El presente contrato de tratamiento de datos forma parte integral del contrato de licencia de usuario final de Kaspersky («contrato de licencia») sobre la prestación de Kaspersky Adaptive Online Training Platform («producto») entre:

Kaspersky Lab Switzerland GmbH,
ubicado en la dirección: Bahnhofstrasse 100, 8001 Zúrich, Suiza[2]

- *El encargado del tratamiento de los datos-*

y

Cliente

- El responsable de los datos -

Apartado 1 Propósito y duración del contrato

1. Propósito del contrato

El propósito del contrato se establece en el **contrato de licencia por escrito.**

2. Duración del contrato

La duración del contrato se establece en el **contrato de licencia por escrito.**

Apartado 2 Alcance, modo y propósito del tratamiento de los datos; tipos de datos y categorías de interesados; derechos y obligaciones del responsable de los datos

1. Modo y propósito del tratamiento de datos

El propósito de la actividad del encargado del tratamiento de los datos se establece en el **contrato de licencia.**

2. Tipos de datos

Los tipos de datos personales son los siguientes:

- Id. de la empresa (si se proporciona).
- Nombre y apellidos.
- Correo electrónico.

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46 /CE (Reglamento General de Protección de Datos).

[2] Se aplican las definiciones del Reglamento General de Protección de Datos.

- Metadatos de la organización (si el responsable de los datos los proporciona), incluyendo:
    - Departamento.
    - Director.
    - Empleados.
- Acciones registradas en el sistema durante su uso normal, entre las que se incluyen:
    - Contenido al que se ha accedido.
    - Respuestas proporcionadas.
    - Tiempo transcurrido.
    - Puntuaciones de autoevaluaciones.
    - Puntuación de finalización.
    - Comentarios y valoraciones.
    - Contenido creado.

3. Categorías de interesados

Las categorías de interesados son las siguientes:
(I) Empleados del responsable de los datos que trabajan con la plataforma, produciendo contenido, aprendiendo y/o accediendo a información sobre la formación.
(II) Clientes del responsable de los datos que hayan adquirido acceso a la plataforma a través de este.
(III) Clientes del responsable de los datos que hayan adquirido acceso a la plataforma a través de este.

Apartado 3 Derecho a instrucción del responsable de los datos

El encargado del tratamiento de los datos puede tratar los datos personales solo con base en instrucciones documentadas facilitadas por el responsable de los datos, incluso si se tratan de transferencias de datos personales a un tercer país o una organización internacional, a menos que contravengan lo exigido por la legislación de la Unión Europea o del Estado miembro a la que está sujeto el encargado del tratamiento. En tal caso, el encargado del tratamiento deberá informar al responsable de los datos de dicho requisito legal antes de llevar a cabo el tratamiento, a menos que esa ley prohíba dicha información por motivos importantes de interés público.

El encargado del tratamiento publicará todas las instrucciones por escrito (por ejemplo, a través de correo electrónico). Si las instrucciones se emiten de forma verbal como excepción, el responsable de los datos deberá confirmarlas adecuadamente por escrito (por ejemplo, a través de correo electrónico).

El encargado del tratamiento deberá informar inmediatamente al responsable de los datos si cree que alguna instrucción infringe el RGPD u otras disposiciones de protección de datos de la Unión Europea o los Estados miembros.

Apartado 4 Obligación de confidencialidad/secreto

El encargado del tratamiento de los datos garantizará que las personas autorizadas para tratar los datos personales se sometan al carácter confidencial o se comprometan a cumplir con las obligaciones reglamentarias aplicables relativas a la confidencialidad.

Apartado 5 Medidas de seguridad técnicas y organizativas para el tratamiento de conformidad con el Artículo 32 Reglamento General de Protección de Datos

El encargado del tratamiento de los datos tomará todas las medidas técnicas y organizativas necesarias de conformidad con el Artículo 32 del RGPD. Estas se describen en detalle en el **anexo 1**.

Las medidas técnicas y organizativas están sometidas al progreso y desarrollo técnicos. Durante la vigencia del presente contrato, las medidas técnicas y organizativas tomadas se ajustarán continuamente a los requisitos del contrato y el encargado del tratamiento de los datos deberá mejorarlas aún más de acuerdo con este contrato y el progreso tecnológico. El nivel de protección no deberá ser inferior a las medidas técnicas y organizativas especificadas en este documento y en el **anexo 1**.

El encargado del tratamiento acepta documentar por escrito y notificar al responsable de los datos sobre cualquier cambio sustancial en las medidas técnicas y organizativas que tenga un impacto significativo en el nivel de seguridad garantizado como complemento del **anexo 1**. Dicha documentación también puede llevarse a cabo de forma electrónica.

Apartado 6 Participación de otros encargados del tratamiento de los datos

El encargado del tratamiento de los datos puede colaborar con otros encargados del tratamiento. Cualquier otro encargado del tratamiento de los datos con el que se colabore en el momento de celebrar el presente contrato figurará en la anexo 2 del mismo. El encargado del tratamiento deberá informar al responsable de los datos por escrito, incluyendo la forma electrónica, sobre cualquier cambio previsto relacionado con la adición o sustitución de otros encargados del tratamiento. El responsable de los datos puede oponerse a dichos cambios.

Si el encargado del tratamiento de los datos colaborara con terceros para llevar a cabo actividades de tratamiento específicas en nombre del responsable de los datos, a dichos terceros se les impondrán las mismas obligaciones de protección de datos establecidas en el contrato u otras disposiciones legales entre el responsable de los datos y el encargado de su tratamiento, tal y como se menciona en el presente contrato, por medio de un contrato u otra disposición legal de acuerdo con la legislación de la Unión Europea o del Estado miembro. En particular se les impondrá la obligación de proporcionar las garantías suficientes para implementar las medidas técnicas y organizativas apropiadas, de tal modo que el tratamiento cumpla con los requisitos del RGPD. Cuando los terceros no cumplan con sus obligaciones de protección de datos, el encargado del tratamiento inicial seguirá siendo el responsable directo ante el responsable de los datos por dichos incumplimientos.

Apartado 7 Deber de cooperar y proporcionar asistencia

Teniendo en cuenta la naturaleza del tratamiento, el encargado del tratamiento deberá proporcionar asistencia al responsable de los datos, en la medida de lo posible, a través las medidas técnicas y organizativas adecuadas para cumplir con las obligaciones del responsable de los datos relativas a la respuesta a solicitudes para ejercer los derechos de los interesados indicado en el Capítulo III de el RGPD (teniendo en cuenta los derechos de los interesados con respecto a la transparencia, el derecho de acceso, el derecho de rectificación, el derecho de borrado («derecho

al olvido»), el derecho a la restricción del tratamiento, la obligación de notificación con respecto a la rectificación o borrado de los datos personales o la restricción del tratamiento, el derecho de portabilidad de datos, el derecho de oposición y el derecho sobre la toma de decisiones individuales automatizadas).

Apartado 8 Apoyo en el cumplimiento de las obligaciones del responsable de los datos

El encargado del tratamiento de los datos deberá proporcionar asistencia al responsable de los mismos con el fin de garantizar que se cumplan las obligaciones en virtud de los Artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información de la que dispone el responsable de los datos (deberá garantizar la seguridad del tratamiento; notificar posibles filtraciones de datos personales a la autoridad supervisora; comunicar posibles filtraciones de datos personales a los interesados; evaluar el impacto de protección de datos; previa consulta).

Apartado 9 Eliminación y devolución de datos personales

A menos que se apliquen períodos de retención legales u de otro tipo, el encargado del tratamiento de los datos deberá proceder con los datos personales utilizados de la siguiente manera una vez finalizado el presente contrato: a solicitud del cliente, el encargado del tratamiento deberá entregar los datos personales al responsable de los datos en un formato legible y editable y eliminar cualquier copia existente, a menos que el responsable solicite al encargado del tratamiento que elimine los datos personales.

Si no se recibe ninguna solicitud por parte del responsable de los datos, los datos personales se deberán eliminar transcurridos 90 días de la finalización del contrato con el cliente.

Apartado 10 Prueba de obligaciones y asistencia en inspecciones

El encargado del tratamiento deberá poner a disposición del responsable de los datos toda la información necesaria para demostrar que cumple con las obligaciones establecidas en el Artículo 28 del RGPD. Asimismo, permitirá y contribuirá a las auditorías (inspecciones) que lleve a cabo el responsable de los datos u otros auditores en nombre de este último.

Apartado 11 Otras estipulaciones

Si el encargado del tratamiento es incapaz de cumplir con el propósito del contrato, tal y como está establecido en el apartado 1 del presente contrato, y este se viera comprometido como resultado de un embargo, incautación o procedimientos de insolvencia o liquidación, o como resultado de otros eventos o medidas tomadas por terceras partes, el encargado del tratamiento deberá ponerlo en conocimiento del responsable de los datos inmediatamente. El encargado del tratamiento deberá notificar de inmediato a todas las partes involucradas que el derecho a disponer de los datos recae exclusivamente sobre el responsable de los mismos.

En caso de posibles discrepancias entre el presente contrato y el **contrato de licencia**, las disposiciones del presente contrato precederán a las disposiciones del **contrato de licencia**.

El contrato se regirá por la legislación del Estado miembro de establecimiento del responsable de los datos.

Si partes individuales de este contrato se declararan nulas, esto no afectará a la validez de las partes restantes.

Cualquier modificación en el presente contrato, incluida su rescisión y cualquier modificación a esta cláusula, deberá hacerse por escrito, lo que también incluye la forma electrónica.

[**Lugar**], a [**fecha**] [**Lugar**], a [**fecha**].

_____ _____

- El encargado del tratamiento de los datos - *- El responsable de los datos -*

Anexo 1 Medidas técnicas y organizativas de conformidad con el Artículo 32 del RGPD

Anexo 2 Otros encargados del tratamiento de los datos

Anexo 1

Medidas técnicas y organizativas de conformidad con el Artículo 32 del RGPD

Teniendo en cuenta

- el estado de la técnica,
- los costes de implementación,
- la naturaleza, el alcance, el contexto
- y los propósitos del tratamiento,
- así como el riesgo de una probabilidad y gravedad variables para los derechos y libertades de las personas físicas,

el encargado del tratamiento de los datos deberá implementar medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo.

Al evaluar el nivel apropiado de seguridad, se deberán tener en cuenta, sobre todo, los riesgos que presenta el tratamiento, en particular la destrucción accidental o ilegal; la pérdida, la alteración o la divulgación: o el acceso no autorizado a los datos personales transmitidos, almacenados o tratados de otro modo.

El encargado del tratamiento deberá cumplir con las siguientes medidas:

Organización de la seguridad de la información

- Se asegurará de nombrar a uno o más jefes de seguridad, responsables de la coordinación y monitorización de las reglas y procedimientos relativos a la seguridad.
- El personal con acceso a los datos del cliente quedará sujeto a las obligaciones relativas a la confidencialidad.
- Se asegurará de realizar una evaluación de riesgos antes de procesar los datos personales o ejecutar los servicios.

Gestión de activos

- Se mantendrá un inventario de todos los activos (qué datos personales se almacenan). El acceso a los inventarios de dichos soportes quedará restringido al personal autorizado.
- Los datos personales se clasificarán para ayudar a identificarlos y para permitir que su acceso quede restringido a las personas adecuadas.
- Será necesaria la obtención de una autorización especial antes de almacenar los datos personales en dispositivos móviles, de acceder remotamente a los datos personales o de tratar los mismos fuera de las instalaciones de la empresa.

Seguridad de Recursos Humanos

- La empresa informará a su personal sobre los procedimientos de seguridad relevantes y sobre sus correspondientes funciones.
- La empresa informará asimismo a su personal sobre las posibles consecuencias de infringir las normas y procedimientos de seguridad.
- La empresa realizará formaciones sobre la seguridad de datos personales.

Seguridad física y medioambiental

- La empresa limitará el acceso a las instalaciones donde se encuentran los sistemas de información en los que se tratan los datos personales a aquellas personas que estén autorizadas:
    - Se proporcionará un servicio de seguridad 24 h, 7 días a la semana, compuesto por guardias de seguridad.
    - El acceso al perímetro estará controlado por un sistema de tarjetas de acceso electrónicas.
    - Se utilizará un molinete con tarjeta de proximidad para todos los puntos de acceso.
    - Los empleados deberán llevar consigo el identificador de la empresa.
    - Los visitantes se registrarán y deberán llevar identificadores de visitante, además de ir acompañados durante su visita.
    - Todos los accesos al perímetro y zonas protegidas estarán monitorizadas con sistemas de CCTV, a su vez monitorizados por guardias de seguridad.
- La empresa conservará registros de los soportes entrantes y salientes, el tipo de soporte, el remitente/destinatarios autorizados, la fecha y hora, y el número de soportes.
- Se implementarán diversos sistemas estándar en el sector para una protección ante la pérdida de datos debido a un fallo en la alimentación o a una interferencia de líneas.
- Se implementarán procesos estándar en el sector para eliminar los datos personales cuando ya no sean necesarios.

Administración de comunicaciones y operaciones

- La empresa conservará los documentos de seguridad que describen sus medidas de seguridad, los procesos relevantes y las responsabilidades del personal que tiene acceso a los datos personales.
- Las copias de los datos personales y de los procesos de recuperación de datos se almacenarán en un lugar diferente de donde se ubica el equipo informático principal que procesa dichos datos.
- Se implementarán controles antimalware para ayudar a evitar que un software malicioso pueda acceder de forma no autorizada a los datos personales, incluyendo aquellos softwares maliciosos que se originan a partir de redes públicas.
- Los datos de los clientes transmitidos a través de redes públicas deberán estar cifrados.
- La empresa registrará los accesos y uso de los sistemas de información que contienen datos personales, registrando así el identificador de acceso, la hora, si la autorización ha sido concedida o rechazada y la actividad relevante.

Control de accesos

- La empresa conservará y mantendrá actualizado un registro del personal con autorización para acceder a los sistemas que contienen datos personales.
- La empresa identificará al personal que pueda otorgar, alterar o cancelar el acceso autorizado a los datos y recursos.
- La empresa se asegurará de que, en caso de que más un individuo tenga acceso a los sistemas que contienen datos personales, dichos individuos tengan identificadores o inicios de sesión diferentes.
- El personal de asistencia técnica únicamente tendrá acceso a los datos personales cuando sea necesario.
- La empresa restringirá el acceso a los datos personales únicamente a aquellas personas que requieran de dicho acceso para llevar a cabo su trabajo.

- La empresa implementará un control de acceso en función de las responsabilidades.
- El personal deberá ser instruido para cerrar las sesiones administrativas al abandonar los controles de las instalaciones o cuando los ordenadores quedan desatendidos por cualquier otro motivo.
- Las contraseñas se almacenarán de tal forma que sean ininteligibles durante su vigencia.
- La empresa utilizará prácticas estándar en el sector para la identificación y autenticación de usuarios que intentan acceder a los sistemas de información.
- La empresa deberá contar con una política de contraseñas que prohíba que se estas se compartan, que establezca las instrucciones que hay que seguir si una contraseña se divulga, y que requiera que se modifiquen las contraseñas de forma periódica y que se cambien las contraseñas predeterminadas.
- La política de contraseñas de la empresa deberá establecer los requisitos de complejidad de las mismas.
- Todas las contraseñas se almacenarán mediante un algoritmo de cifrado unidireccional y nunca se transmitirán sin cifrar.
- La empresa deberá disponer de controles para evitar que cualquier individuo se otorgue derechos de acceso que no se le han asignado para obtener acceso a los datos de los clientes a los que no están autorizados a acceder.
- El canal de la red interna de la empresa deberá estar protegido mediante la implementación de cortafuegos.
- Todas las trasferencias de datos entre la empresa, el departamento legal, las entidades y socios y los clientes deberán estar protegidas mediante el protocolo TLS/SSL.

Gestión de incidentes en la seguridad de la información

- La empresa deberá llevar un registro de violaciones de seguridad con una descripción de la misma, el periodo de tiempo, las consecuencias de la violación, el nombre del informante y de la persona a la que se informó sobre la violación, y el procedimiento para la recuperación de datos.

Gestión de vulnerabilidades

- Los recursos de información de la empresa se deberán comprobar periódicamente mediante exploraciones de vulnerabilidad.
- La empresa deberá realizar pruebas de penetración en recursos de información, además de auditorías de seguridad.

Anexo 2

Otros encargados del tratamiento de los datos

Nombre y dirección del encargado del tratamiento	Objeto/motivo de la subcontratación	Opcional: fecha de celebración del contrato de subcontratación
Amazon Web Services EMEA SARL 5 rue Plaetis L-2338 Luxemburgo	Proveedor de centros de datos, así como de servicios de software y energía de ordenadores virtuales en la nube. Amazon Web Services EMEA SARL. Regiones en las que se utilizarán los datos del usuario final: Germany – AWS Region Frankfurt (EU)	
Area9 Technologies ApS Núm. de registro de la empresa: 34489343 Galionsvej 37, DK 1437 Copenhague K, Dinamarca	Soporte de TI y alojamiento de servidores	
Area9 Labs ApS Núm. de registro de la empresa: 25167406 Galionsvej 37, DK 1437 Copenhague K, Dinamarca	Soporte de TI y alojamiento de servidores	
Area9 Innovation ApS Núm. de registro de la empresa: 36921897 Galionsvej 37, DK 1437 Copenhague K, Dinamarca	Soporte de TI y alojamiento de servidores	
Area9 Lyceum ApS Núm. de registro de la empresa: 39079976 Galionsvej 37, DK 1437 Copenhague K, Dinamarca	Soporte de TI y alojamiento de servidores	
Atlassian B.V. c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, CA 94104	Sistema de asistencia informática	
AO Kaspersky Lab, 39A/2 Leningradskoe Shosse Moscú, 125212 Federación de Rusia	Proporciona el acceso inicial al servicio, registro de administradores.	