Vereinbarung zwischen Verantwortlichem und Verarbeiter

gemäß Artikel 28 Allgemeine Datenschutzverordnung[1] (*DSGVO*)

Diese Datenverarbeitungsvereinbarung ist ein wesentlicher Bestandteil der Kaspersky Endbenutzer-Lizenzvereinbarung („Lizenzvereinbarung“) zur Bereitstellung der Kaspersky Adaptive Online Training Platform („Produkt“) zwischen:

Kaspersky Lab Switzerland GmbH,
unter der Adresse: Bahnhofstrasse 100, 8001 Zürich, Schweiz[2]

- *Verarbeiter*-

und

Kunde

- *Verantwortlicher* -

Abschnitt 1 Zweck und Dauer der Vereinbarung

1. Zweck der Vereinbarung

Der Zweck der Vereinbarung ist in der schriftlichen **Lizenzvereinbarung festgelegt.**

2. Dauer der Vereinbarung

Die Dauer der Vereinbarung ist in der schriftlichen **Lizenzvereinbarung festgelegt.**

Abschnitt 2 Umfang, Art und Zweck der Datenvereinbarung, Datentypen und Kategorien der betroffenen Personen, Rechte und Verpflichtungen des für die Verarbeitung Verantwortlichen

1. Art und Weise und Zweck der Datenverarbeitung

Der Tätigkeitszweck des Verarbeiters ist in der **Lizenzvereinbarung festgelegt.**

2. Datenarten

Die Arten von personenbezogenen Daten sind:

- Firmen-ID (falls angegeben)
- Vor-und Nachname
- E-Mail

[1]Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Austausch solcher Daten und zur Aufhebung der Richtlinie 95/46/EG (Allgemeine Datenschutzverordnung).

[2] Es gelten die Definitionen der Allgemeinen Datenschutzverordnung.

- Organisatorische Metadaten (wie vom Datenverantwortlichen bereitgestellt), einschließlich:
    - Abteilung
    - Manager
    - Mitarbeiter
- Erfasste Aktionen innerhalb des Systems während der regelmäßigen Verwendung, einschließlich:
    - Zugriff auf Inhalte
    - Antworten
    - Aufgewendete Zeit
    - Selbstbewertungsergebnisse
    - Abschlussergebnis
    - Kommentare und Feedback
    - Erstellter Inhalt

3. Kategorien betroffener Personen

Die Kategorien der betroffenen Personen sind:
(i) Mitarbeiter des Datenverantwortlichen, die mit der Plattform arbeiten, Inhalte erstellen, lernen und / oder auf Informationen zum Lernen zugreifen.
(ii) Kunden des Datenverantwortlichen, die über den Datenverantwortlichen Zugang zur Plattform erworben haben.
(iii) Kunden des Datenverantwortlichen, die über den Datenverarbeiter Zugriff auf die Plattform erworben haben.

Abschnitt 3 Weisungsrecht des für die Verarbeitung Verantwortlichen

Der Verarbeiter darf die personenbezogenen Daten nur nach dokumentierten Anweisungen des für die Verarbeitung Verantwortlichen verarbeiten, auch im Hinblick auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, es sei denn, dies ist nach dem Recht der Union oder des Mitgliedstaates, dem der Verarbeiter unterliegt, erforderlich. In einem solchen Fall informiert der Verarbeiter den Verantwortlichen über diese gesetzliche Anforderung vor der Verarbeitung, es sei denn, dieses Gesetz verbietet diese Informationen aus wichtigen Gründen des öffentlichen Interesses.

Der Verarbeiter erteilt alle Anweisungen in Textform (z. B. per E-Mail). Wenn Anweisungen ausnahmsweise mündlich erteilt werden, müssen sie von dem für die Verarbeitung Verantwortlichen in Textform (z. B. per E-Mail) in angemessener Weise bestätigt werden.

Der Verarbeiter hat den für die Verarbeitung Verantwortlichen unverzüglich zu informieren, wenn nach seiner Auffassung eine Anweisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder des Mitgliedstaates verstößt.

Abschnitt 4 Vertraulichkeitsverpflichtung / Geheimhaltungspflicht

Der Verarbeiter stellt sich, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen.

Abschnitt 5 Verarbeitung von Sicherheits- / technischen und organisatorischen Maßnahmen gemäß Artikel 32 der Allgemeinen Datenschutzverordnung

Der Verarbeiter trifft alle technischen und organisatorischen Maßnahmen, die gemäß Artikel 32 DSGVO erforderlich sind. Diese sind in **Anlage 1** ausführlich dargestellt.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischem Fortschritt und der technischen Entwicklungen. Für die Dauer dieser Vereinbarung werden die getroffenen technischen und organisatorischen Maßnahmen kontinuierlich an die Anforderungen der Vereinbarung angepasst und vom Verarbeiter gemäß dieser Vereinbarung und dem technologischen Fortschritt weiterentwickelt. Das Schutzniveau darf die hier und in **Anlage 1** angegebenen technischen und organisatorischen Maßnahmen nicht unterschreiten.

Der Verarbeiter verpflichtet sich, wesentliche Änderungen der technischen und organisatorischen Maßnahmen, die erhebliche Auswirkungen auf das garantierte Sicherheitsniveau haben, zusätzlich zu **Anlage 1** schriftlich zu dokumentieren und den für die Verarbeitung Verantwortlichen darüber zu informieren. Eine solche Dokumentation kann auch in elektronischer Form erfolgen.

Abschnitt 6 Beauftragung eines anderen Verarbeiters

Der Verarbeiter kann einen anderen Verarbeiter beauftragen. Jeder andere zum Zeitpunkt des Abschlusses der Vereinbarung beauftragte Verarbeiter ist in Anlage 2 zu dieser Vereinbarung aufgeführt. Der Verarbeiter informiert den Controller schriftlich, auch in elektronischer Form, über beabsichtigte Änderungen in Bezug auf das Hinzufügen oder Ersetzen anderer Verarbeiter. Der Verantwortliche hat die Möglichkeit, solchen Änderungen zu widersprechen.

Wenn der Verarbeiter einen anderen Verarbeiter mit der Durchführung bestimmter Verarbeitungsaktivitäten im Auftrag des für die Verarbeitung Verantwortlichen beauftragt, werden diesem anderen Verarbeiter dieselben Datenschutzverpflichtungen auferlegt, wie sie im Vertrag oder in einem anderen Rechtsakt zwischen dem für die Verarbeitung Verantwortlichen und dem Verarbeiter festgelegt sind, auf den in dieser Vereinbarung Bezug genommen wird, in Form eines Vertrags oder eines anderen Rechtsakts nach dem Gesetz der Union oder des Mitgliedstaats, insbesondere mit ausreichenden Garantien, um geeignete technische und organisatorische Maßnahmen in einer Weise umzusetzen, dass die Verarbeitung den Anforderungen der DSGVO entspricht. Wenn der andere Verarbeiter seinen Datenschutzverpflichtungen nicht nachkommt, haftet der Datenverarbeiter gegenüber dem Datenverantwortlichen weiterhin uneingeschränkt für die Erfüllung der Verpflichtungen dieses anderen Verarbeiters.

Abschnitt 7 Mitwirkungspflicht / Unterstützungspflicht

Unter Berücksichtigung der Art der Verarbeitung unterstützt der Verarbeiter den für die Verarbeitung Verantwortlichen durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, um die Verpflichtung des für die Verarbeitung Verantwortlichen zu erfüllen, auf Anfragen zur Ausübung der in Kapitel III von die DSGVO (unter Berücksichtigung der Rechte der betroffenen Person in Bezug auf Transparenz, Zugangsrecht, Recht auf Berichtigung, Recht auf Löschung („Recht auf Vergessenwerden“), Recht auf Einschränkung der Verarbeitung, Meldepflicht in Bezug auf Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der

Verarbeitung, Recht auf Datenübertragbarkeit, Recht auf Widerspruch, Recht auf automatisierte individuelle Entscheidungsfindung).

Abschnitt 8 Unterstützung bei der Erfüllung der Verpflichtungen des Verantwortlichen

Der Verarbeiter unterstützt den für die Verarbeitung Verantwortlichen bei der Sicherstellung der Einhaltung der Verpflichtungen gemäß den Artikeln 32 bis 36 unter Berücksichtigung der Art der Verarbeitung und der dem Verarbeiter zur Verfügung stehenden Informationen (Gewährleistung der Sicherheit der Verarbeitung; Benachrichtigung über einen Verstoß gegen personenbezogene Daten an die Aufsichtsbehörde; Kommunikation eines Verstoßes gegen personenbezogene Daten an die betroffene Person; Folgenabschätzung zum Datenschutz; vorherige Konsultation).

Abschnitt 9 Löschung und Rückgabe von personenbezogenen Daten

Sofern keine gesetzlichen oder sonstigen Aufbewahrungsfristen gelten, wird der Verarbeiter nach Abschluss der Vereinbarung mit den verwendeten personenbezogenen Daten wie folgt vorgehen: Auf Wunsch des Kunden übergibt der Verarbeiter diese personenbezogenen Daten in lesbarer und bearbeitbarer Form an den Verantwortlichen und löscht vorhandene Kopien, es sei denn, der Verantwortliche fordert den Verarbeiter auf, die personenbezogenen Daten zu löschen.

Wenn keine Anfrage vom Verantwortlichen eingeht, werden personenbezogene Daten 90 Tage nach Ende der Vereinbarung mit dem Kunden gelöscht.

Abschnitt 10 Nachweis von Verpflichtungen und Unterstützung bei Inspektionen

Der Verarbeiter stellt dem für die Verarbeitung Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Artikel 28 DSGVO festgelegten Verpflichtungen erforderlich sind. Er ermöglicht Audits und trägt zu Audits bei, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen, vom Verantwortlichen beauftragten Prüfer, durchgeführt werden.

Abschnitt 11 Sonstiges

Wenn die Erfüllung des in Abschnitt 1 dieser Vereinbarung festgelegten Vertragszwecks seitens des Verarbeiters durch Pfändung oder Beschlagnahme oder durch ein Insolvenz- oder Vergleichsverfahren oder durch andere von Dritten getroffene Ereignisse oder Maßnahmen gefährdet ist, hat der Verarbeiter den Verantwortlichen unverzüglich zu benachrichtigen. Der Verarbeiter hat alle Beteiligten unverzüglich darüber zu informieren, dass das Verfügungsrecht über die Daten ausschließlich beim Verantwortlichen liegt.

Bei möglichen Abweichungen zwischen dieser Vereinbarung und der **Lizenzvereinbarung** haben die Bestimmungen dieser Vereinbarung Vorrang vor den Bestimmungen der **Lizenzvereinbarung**.

Die Vereinbarung unterliegt dem Recht des EU-Staates, in dem der für die Verarbeitung Verantwortliche niedergelassen ist.

Sollten einzelne Teile dieser Vereinbarung ungültig sein, so wird hierdurch die Gültigkeit der übrigen Teile der Vereinbarung nicht berührt.

Jede Änderung dieser Vereinbarung, einschließlich ihrer Kündigung und jede Änderung dieser Klausel, muss schriftlich erfolgen. „*Schriftlich*" umfasst auch die elektronische Form.

[**Ort**], am [**Datum**] [**Ort**], am [**Datum**].

_____ _____

- Verarbeiter - *- Verantwortlicher -*

Anlage 1 Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Anlage 2 Andere Verarbeiter

Anlage 1

Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Unter Berücksichtigung

- des Standes der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, des Kontexts und
- der Zwecke der Verarbeitung sowie
- des Risikos unterschiedlicher Wahrscheinlichkeiten und Schweregrade der Rechte und Freiheiten natürlicher Personen,

hat der Verarbeiter angemessene technische und organisatorische Maßnahmen durchzuführen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

Bei der Bewertung des angemessenen Sicherheitsniveaus sind insbesondere die Risiken zu berücksichtigen, die durch die Verarbeitung, insbesondere durch zufällige(n) oder unrechtmäßige(n) Zerstörung, Verlust, Veränderung, die unbefugte Weitergabe von oder den Zugriff auf übertragene, gespeicherte oder anderweitig verarbeitete personenbezogene Daten entstehen.

Der Verarbeiter hält die folgenden Maßnahmen ein:

Organisation der Informationssicherheit

- Ein Sicherheitsbeauftragter oder mehre Sicherheitsbeauftragte wurde(n) ernannt, der / die für die Koordinierung und Überwachung der Sicherheitsregeln und -verfahren verantwortlich ist / sind
- Mitarbeiter mit Zugriff auf Kundendaten unterliegen den Verpflichtungen zur Vertraulichkeit.
- Vor der Verarbeitung der personenbezogenen Daten oder der Einführung der Dienste wurde eine Risikobewertung durchgeführt.

Verwaltung der Vermögenswerte

- Das Inventar aller Vermögenswerte (in denen / mit denen personenbezogene Daten gespeichert werden) wird geführt. Der Zugriff auf Bestände solcher Medien ist auf Mitarbeiter beschränkt, die zu einem solchen Zugriff berechtigt sind.
- Personenbezogene Daten werden klassifiziert, um sie leichter identifizieren zu können und um den Zugriff darauf angemessen einzuschränken
- Vor dem Speichern personenbezogener Daten auf tragbaren Geräten, dem Remotezugriff auf personenbezogene Daten oder der Verarbeitung personenbezogener Daten außerhalb der Einrichtungen des Unternehmens ist eine spezielle Genehmigung erforderlich

Sicherheit der Mitarbeiter

- Das Unternehmen informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Rollen.
- Das Unternehmen informiert seine Mitarbeiter auch über mögliche Folgen eines Verstoßes gegen die Sicherheitsregeln und -verfahren
- Das Unternehmen führt Schulungen zur Sicherheit personenbezogener Daten durch

Physische Sicherheit und Umgebungssicherheit

- Das Unternehmen beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme zur Verarbeitung personenbezogener Daten befinden, auf identifizierte autorisierte Personen:
    - Der 7x24-Sicherheitsdienst wird von Sicherheitspersonal bereitgestellt
    - Der Zugang zum Umkreis wird durch das elektronische Zugangskartensystem gesteuert
    - Das Drehkreuz wird mit kontaktlosen Karten an allen Eingängen betrieben
    - Die Mitarbeiter müssen das Firmenabzeichen tragen
    - Besucher werden registriert und müssen Besucherausweise tragen. Besucher werden während ihres Besuchs begleitet
    - Alle Zugänge zum Außenbereich und zu Sicherheitsbereichen werden durch Überwachungskameras kontrolliert, die vom Sicherheitsdienst überwacht werden
- Das Unternehmen führt Aufzeichnungen über eingehende und ausgehende Medien, einschließlich der Art der Medien, des autorisierten Absenders / Empfängers, des Datums und der Uhrzeit sowie der Anzahl der Medien.
- Eine Vielzahl von Branchenstandardsystemen wurde implementiert, um vor Datenverlust aufgrund von Stromausfällen oder einer Leitungsstörung zu schützen.
- Es wurden Branchenstandardverfahren zum Löschen personenbezogener Daten implementiert, wenn diese nicht mehr benötigt werden.

Kommunikations- und Betriebsmanagement

- Das Unternehmen führt Sicherheitsdokumente, in denen seine Sicherheitsmaßnahmen sowie die relevanten Verfahren und Verantwortlichkeiten seiner Mitarbeiter beschrieben sind, die Zugriff auf personenbezogene Daten haben.
- Kopien personenbezogener Daten und Datenwiederherstellungsverfahren werden an einem anderen Ort gespeichert als die Hauptcomputerausrüstung, die die personenbezogenen Daten verarbeitet.
- Anti-Malware-Kontrollen wurden implementiert, um zu verhindern, dass schädliche Software unbefugten Zugriff auf personenbezogene Daten erhält, einschließlich schädlicher Software, die aus öffentlichen Netzwerken stammt.
- Kundendaten, die über öffentliche Netzwerke übertragen werden, sind verschlüsselt.
- Unternehmensprotokolle, Zugriff und Nutzung von Informationssystemen, die personenbezogene Daten enthalten, Registrierung der Zugriffs-ID, Zeit, erteilte oder verweigerte Berechtigung sowie relevante Aktivitäten.

Zugriffskontrolle

- Das Unternehmen führt und aktualisiert eine Aufzeichnung der Mitarbeiter, die zum Zugriff auf Systeme mit Kundendaten berechtigt sind.
- Das Unternehmen identifiziert diejenigen Mitarbeiter, die berechtigten Zugriff auf Daten und Ressourcen gewähren, ändern oder sperren können.
- Das Unternehmen stellt sicher, dass wenn mehr als eine Person Zugriff auf Systeme mit Kundendaten hat, die Personen separate Kennungen / Anmeldungen haben.
- Mitarbeiter des technischen Supports dürfen nur auf personenbezogene Daten zugreifen, wenn dies erforderlich ist.
- Das Unternehmen beschränkt den Zugriff auf personenbezogene Daten nur auf diejenigen Personen, die einen solchen Zugriff benötigen, um ihre Arbeitsaufgaben wahrzunehmen.
- Das Unternehmen implementiert rollen-basierte Zugriffskontrolle

- Die Mitarbeiter wurde angewiesen, administrative Sitzungen zu deaktivieren, wenn die Betriebskontrollen verlassen werden oder wenn Computer anderweitig unbeaufsichtigt bleiben.
- Passwörter werden so gespeichert, dass sie während ihrer Gültigkeit nicht zu entziffern sind.
- Das Unternehmen verwendet Branchenstandardverfahren, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen.
- Das Unternehmen hat eine Passwortrichtlinie festgelegt, die die Weitergabe von Passwörtern untersagt, regelt, was zu tun ist, wenn ein Passwort veröffentlicht wird und die regelmäßige Änderung von Passwörtern sowie die Änderung von Standardpasswörtern erfordert.
- Die Passwortrichtlinie des Unternehmens definiert die Anforderungen an die Passwortkomplexität.
- Alle Passwörter werden mithilfe eines einseitigen Hash-Algorithmus gespeichert und werden niemals unverschlüsselt übermittelt.
- Das Unternehmen verfügt über Kontrollen, um zu verhindern, dass Personen Zugriffsrechte übernehmen, denen sie nicht zugewiesen wurden, um Zugriff auf Kundendaten zu erhalten, auf die sie keinen Zugriff haben
- Der unternehmensinterne Netzwerkkanal wird durch die Implementierung von Firewalls geschützt.
- Alle Datenübertragungen zwischen dem Unternehmen, juristischen Personen sowie Partnern und Kunden sind durch das TLS / SSL-Protokoll geschützt.

Informationen zum Management von Sicherheitsvorfällen

- Das Unternehmen führt Aufzeichnungen über Sicherheitsverstößen mit einer Beschreibung des Verstoßes, des Zeitraums, der Folgen des Verstoßes, des Namens des Berichtenden und wem der Verstoß gemeldet wurde sowie des Verfahrens zur Wiederherstellung von Daten.

Schwachstellen-Management

- Die Informationsressourcen des Unternehmens werden regelmäßig von Schwachstellen-Scannern überprüft
- Das Unternehmen führt Informationsressourcen und Sicherheitsprüfungen für Penetrationstests durch

Anlage 2

Andere Verarbeiter

Name und Anschrift eines anderen Verarbeiters	Gegenstand der Vergabe von Unteraufträgen	Wahlweise: Datum des Vertragsabschlusses bezüglich der Vergabe von Unteraufträgen
Amazon Web Services EMEA SARL 5 rue Plaetis L-2338 Luxemburg	Rechenzentrumsanbieter und Cloud-Anbieter von Strom- und Softwarediensten für virtuelle Computer. EMEA SARL-Regionen von Amazon Web Services, zur Verwendung von Endbenutzerdaten: Deutschland - AWS Region Frankfurt (EU)	
Area9 Technologies ApS Firmenreg.Nr.: 34489343 Galionsvej 37, DK 1437 Kopenhagen K, Dänemark	IT-Support und Server-Hosting	
Area9 Labs ApS Firmenreg.Nr.: 25167406 Galionsvej 37, DK 1437 Kopenhagen K, Dänemark	IT-Support und Server-Hosting	
Area9 Innovation ApS Firmenreg.Nr.: 36921897 Galionsvej 37, DK 1437 Kopenhagen K, Dänemark	IT-Support und Server-Hosting	
Area9 Lyceum ApS Firmenreg.Nr.: 39079976 Galionsvej 37, DK 1437 Kopenhagen K, Dänemark	IT-Support und 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, Moskau, 125212, Russische Föderation	Bereitstellung des ersten Zugriffs auf den Dienst, Registrierung von Administratoren	