Auftragsverarbeitungsvertrag (AVV)

Dieser Auftragsverarbeitungsvertrag beschreibt die Bedingungen für die Verarbeitung personenbezogener Daten durch Learned B.V. im Auftrag des Kunden auf Grundlage der zwischen den Parteien geschlossenen SaaS-Vereinbarung. Dieser Auftragsverarbeitungsvertrag ist ein integraler und untrennbarer Bestandteil der für die Plattform von Learned geltenden Allgemeinen Geschäftsbedingungen.

Artikel 1 – Begriffsbestimmungen

1. Der Begriff „AVG“ in diesem Auftragsverarbeitungsvertrag bezeichnet die Datenschutz-Grundverordnung (DSGVO) sowie sämtliche gesetzlichen Vorschriften, die diese künftig ersetzen oder ergänzen.

2. Begriffe, die in der DSGVO definiert sind, haben in diesem Vertrag dieselbe Bedeutung, sofern in diesem Vertrag keine abweichende Definition getroffen wird.

3. Der Kunde gilt als Verantwortlicher im Sinne von Artikel 4 Absatz 7 DSGVO.

4. Learned gilt als Auftragsverarbeiter im Sinne von Artikel 4 Absatz 8 DSGVO.

5. Der Begriff „personenbezogene Daten“ umfasst personenbezogene Daten, die sich auf Mitarbeiter des Verantwortlichen, dessen Kunden und/oder sonstige Geschäftsbeziehungen beziehen. Learned unterscheidet zwischen zwei Kategorien personenbezogener Daten: Systemkritische personenbezogene Daten und Sensible personenbezogene Daten

6. Der Begriff „Unterauftragsverarbeiter“ bezeichnet eine juristische Person, die vom Auftragsverarbeiter im Auftrag und für Rechnung des Auftragsverarbeiters zur Verarbeitung personenbezogener Daten im Rahmen der Leistungserbringung eingeschaltet wird und dabei personenbezogene Daten erhält oder Zugriff darauf hat.

Artikel 2 – Zweck und Mittel der Verarbeitung

1. Der Kunde behält als Verantwortlicher jederzeit die Kontrolle über die personenbezogenen Daten, die er dem Auftragsverarbeiter im Rahmen der Durchführung des SaaS-Vertrags zur Verfügung stellt, einschließlich aller Aktualisierungen, Änderungen, Korrekturen oder Ergänzungen dieser Daten.

2. Der Auftragsverarbeiter erklärt sich damit einverstanden, dass die Zwecke der Verarbeitung personenbezogener Daten ausschließlich vom Kunden in seiner Funktion als Verantwortlicher festgelegt werden. Die Kategorien personenbezogener Daten, betroffene Personen sowie die Zwecke der Verarbeitung sind in Anhang 1 aufgeführt.

3. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich, soweit dies zur Erbringung seiner Dienstleistungen gegenüber dem Kunden erforderlich ist, im Einklang mit den vom Kunden festgelegten Zwecken (gemäß Anhang 1), oder

soweit eine gesetzliche Verpflichtung dies erfordert. Eine Speicherung, Aufbewahrung oder sonstige Verarbeitung personenbezogener Daten zu anderen Zwecken ist ausgeschlossen.

4. Auf diesen Auftragsverarbeitungsvertrag finden die DSGVO (seit 25. Mai 2018), das niederländische Telekommunikationsgesetz sowie sämtliche weiteren einschlägigen europäischen Datenschutzvorschriften Anwendung.

Artikel 3 – Sicherheit

1. Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
   Diese Maßnahmen gewährleisten insbesondere:
   - ein angemessenes Sicherheitsniveau unter Berücksichtigung des Stands der Technik und der Implementierungskosten,
   - die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten.

   Die Maßnahmen umfassen mindestens:
   - Maßnahmen zur Sicherstellung, dass nur autorisiertes Personal Zugriff auf personenbezogene Daten hat;
   - Maßnahmen zum Schutz vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Speicherung, Verarbeitung, Zugriff oder Offenlegung;
   - Maßnahmen zur Identifizierung von Schwachstellen in den eingesetzten Systemen zur Datenverarbeitung.

2. Ohne schriftliche Zustimmung des Kunden darf der Auftragsverarbeiter personenbezogene Daten nicht in einem Staat außerhalb des Europäischen Wirtschaftsraums (EWR) ohne angemessenes Datenschutzniveau verarbeiten lassen oder durch Dritte verarbeiten lassen. Der Kunde darf seine Zustimmung nicht ohne sachlichen Grund verweigern. Der Auftragsverarbeiter stellt sicher, dass geeignete Garantien bestehen, wenn personenbezogene Daten in Länder außerhalb des EWR übertragen werden.

3. Auf Anfrage des Kunden informiert der Auftragsverarbeiter über die getroffenen Sicherheitsmaßnahmen, einschließlich des Standorts der Server oder anderer Systeme, auf denen personenbezogene Daten gespeichert oder verarbeitet werden. Sollte der Kunde die Maßnahmen als unzureichend ansehen, wird der Auftragsverarbeiter geeignete Anpassungen vorschlagen. Der Kunde darf seine Zustimmung zu angemessenen Maßnahmen nicht unbegründet verweigern. Die Kosten für die Umsetzung solcher Maßnahmen trägt der Auftragsverarbeiter.

4. Der Auftragsverarbeiter unterstützt den Kunden bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO, beispielsweise bei der Durchführung einer Datenschutz-Folgenabschätzung (DSFA / DPIA). Learned kann hierfür Kosten auf Basis seiner üblichen Stundensätze berechnen.

Artikel 4 – Einsatz von Unterauftragsverarbeitern

1. Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten einzusetzen. Der Kunde erteilt hiermit seine Zustimmung für die in Anhang 1b aufgeführten Unterauftragsverarbeiter.

2. Während der Zusammenarbeit kann der Auftragsverarbeiter zusätzliche Unterauftragsverarbeiter einsetzen:
    - für systemkritische personenbezogene Daten, sofern dies für die Leistungserbringung erforderlich ist,
    - für sensible personenbezogene Daten nur mit vorheriger schriftlicher Zustimmung des Kunden.

3. Der Auftragsverarbeiter informiert den Kunden mindestens einen Monat vor Einsatz eines neuen Unterauftragsverarbeiters, der sensible personenbezogene Daten verarbeitet. Der Kunde kann innerhalb von 30 Tagen schriftlich und begründet widersprechen, wenn berechtigte Gründe vorliegen. Die Parteien werden in diesem Fall in Konsultation treten, um zu einer gemeinsamen Lösung zu gelangen.

4. Kommt keine Einigung zustande, darf der Auftragsverarbeiter den Unterauftragsverarbeiter einsetzen; der Kunde ist jedoch berechtigt, den Vertrag zum Zeitpunkt des Einsatzes zu kündigen. Erfolgt innerhalb von 30 Tagen kein Widerspruch, gilt die Zustimmung als erteilt.

5. Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter vertraglich gleichwertige Datenschutzpflichten übernehmen.

6. Der Auftragsverarbeiter hat sicherzustellen, dass sich Unterauftragsverarbeiter schriftlich zu Pflichten verpflichten, die den zwischen dem Auftragsverarbeiter und dem Kunden vereinbarten Pflichten entsprechen. So hat der Auftragsverarbeiter beispielsweise in jedem Fall mit Unterauftragsverarbeitern außerhalb der EU Standardvertragsklauseln (SCCs) abgeschlossen.

Artikel 5 – Vertraulichkeit

1. Der Auftragsverarbeiter ist verpflichtet, personenbezogene Daten vertraulich zu behandeln und – außer bei gesetzlicher Verpflichtung – nicht an Dritte weiterzugeben.

2. Der Auftragsverarbeiter stellt sicher, dass Mitarbeiter sowie eingeschaltete Dritte dieser Vertraulichkeitsverpflichtung unterliegen.

3. Der Kunde wird unverzüglich informiert, wenn eine Anfrage auf Offenlegung personenbezogener Daten eingeht.

Artikel 6 – Informations- und Mitwirkungspflichten

1. Der Auftragsverarbeiter wird dem Kunden auf dessen Verlangen sämtliche Auskünfte über die Verarbeitung(en) der personenbezogenen Daten durch den Auftragsverarbeiter oder durch vom Auftragsverarbeiter eingeschaltete Dritte erteilen. Der Auftragsverarbeiter wird die angeforderten Auskünfte so schnell wie möglich, spätestens jedoch innerhalb von sieben (7) Tagen, bereitstellen.

2. Der Auftragsverarbeiter wird auf Verlangen des Kunden in vollem Umfang mitwirken im Falle einer Beschwerde oder Frage einer betroffenen Person beziehungsweise bei Untersuchungen oder Inspektionen durch die Datenschutzbehörde.

3. Wenn der Auftragsverarbeiter unmittelbar von einer betroffenen Person ein Ersuchen auf Auskunft, Berichtigung, Löschung oder Datenübertragbarkeit ihrer personenbezogenen Daten erhält, leitet der Auftragsverarbeiter das Ersuchen unverzüglich, spätestens jedoch innerhalb von zwei (2) Arbeitstagen, an den Kunden weiter.

4. Der Auftragsverarbeiter wird unverzüglich alle angemessenen Weisungen ausführen, die der Kunde dem Auftragsverarbeiter infolge eines Antrags einer betroffenen Person auf Auskunft, Berichtigung, Löschung oder Datenübertragbarkeit personenbezogener Daten erteilt.

5. Der Auftragsverarbeiter wird unverzüglich jede andere angemessene Weisung des Kunden zur Löschung personenbezogener Daten ausführen; hierzu gehören insbesondere Weisungen zur Löschung personenbezogener Daten, deren Aufbewahrungsfrist abgelaufen ist, sowie zur Löschung personenbezogener Daten auf Antrag einer betroffenen Person.

6. Der Auftragsverarbeiter wird den Kunden unverzüglich über jede Änderung in der Organisationsstruktur des Auftragsverarbeiters oder der Kontrolle über den Auftragsverarbeiter informieren, soweit diese einen wesentlichen Einfluss auf die Art und Weise haben, in der die personenbezogenen Daten verarbeitet oder geschützt werden, oder auf die Verpflichtungen des Auftragsverarbeiters aus dieser Vereinbarung.

Artikel 7 – Risikoanalysen und Meldung von Datenschutzverletzungen

1. Der Kunde ist grundsätzlich verantwortlich für die Meldung einer Verletzung des Schutzes personenbezogener Daten (Data Breach) an Aufsichtsbehörden und betroffene Personen.

2. Damit der Kunde dieser Pflicht nachkommen kann, informiert der Auftragsverarbeiter den Kunden innerhalb von 24 Stunden nach Bekanntwerden einer Datenschutzverletzung.

3. Die Meldepflicht besteht in der Meldung der Datenschutzverletzung und der Bereitstellung aller relevanten Informationen, soweit diese Informationen verfügbar sind. Dies umfasst in jedem Fall, jedoch nicht ausschließlich, Folgendes:
    - die (vermutete) Ursache der Datenschutzverletzung;
    - die (bislang bekannten und/oder zu erwartenden) Folgen (für die betroffenen Personen);
    - die (vorgeschlagene) Lösung; und
    - die bereits ergriffenen Maßnahmen.

Artikel 8 – Löschung und Rückgabe personenbezogener Daten

1. Der Auftragsverarbeiter wird unmittelbar nach Beendigung dieser Vereinbarung sämtliche personenbezogenen Daten an den Kunden übergeben und aus seinen Systemen löschen und vernichten beziehungsweise auf Verlangen des Kunden zurückgeben, sofern eine gesetzliche Aufbewahrungspflicht einer solchen Löschung oder Vernichtung nicht entgegensteht. Auf erstes Verlangen des Kunden wird der Auftragsverarbeiter hierfür einen Nachweis erbringen. Nach Ablauf des Backup-Zeitraums von zwölf (12) Monaten werden die Daten endgültig aus der Datenbank gelöscht.

2. Der Auftragsverarbeiter ist verpflichtet, sämtliche personenbezogenen Daten unverzüglich zu vernichten, sobald er diese für die Durchführung des Anschlussvertrags nicht länger zwingend benötigt. Diese Vernichtung darf in keinem Fall später erfolgen als zu dem Zeitpunkt, an dem die gesetzliche Aufbewahrungsfrist für die betreffenden personenbezogenen Daten abgelaufen ist. Auf erstes Verlangen des Kunden wird der Auftragsverarbeiter hierfür einen Nachweis erbringen.

Artikel 9 – Ort der Datenverarbeitung

1. Die Verarbeitung personenbezogener Daten erfolgt innerhalb der Europäischen Union (EU). Die Daten werden in Deutschland gespeichert.

Artikel 10 – Laufzeit und Beendigung

1. Die Vereinbarung kann nur insoweit gekündigt, aufgelöst oder anderweitig beendet werden, wie es in diesem Artikel 10 vorgesehen ist.

2. Diese Vereinbarung tritt am ersten Tag der Unterzeichnung des SaaS-Vertrags durch die Parteien in Kraft und gilt auf unbestimmte Zeit, soweit der Verarbeiter im Rahmen seiner Dienstleistungen für den Kunden personenbezogene Daten verarbeitet. Mit Beendigung der Dienstleistungen des Kunden gegenüber dem Verarbeiter endet diese Vereinbarung kraft Gesetzes.

3. Die Beendigung dieser Vereinbarung entbindet die Parteien ausdrücklich nicht von denjenigen Verpflichtungen, die ihrer Natur nach fortgelten sollen, einschließlich der Bestimmungen über (Haftungs-)Beschränkung, Freistellung, Pflichten des Auftragsverarbeiters hinsichtlich personenbezogener Daten sowie über anwendbares Recht und Streitbeilegung.

Artikel 11 – Schlussbestimmungen

1. Änderungen dieses Vertrags bedürfen der Schriftform.

2. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Die unwirksame Bestimmung wird durch eine Regelung ersetzt, die dem wirtschaftlichen Zweck möglichst nahekommt.

3. Dieser Vertrag unterliegt ausschließlich niederländischem Recht.

4. Gerichtsstand für alle Streitigkeiten ist das Bezirksgericht Utrecht (Niederlande).

Anhang 1a | Übersicht personenbezogener Daten

Kategorien personenbezogener Daten
Learned unterscheidet zwischen zwei verschiedenen Kategorien personenbezogener Daten der betroffenen Personen, nämlich systemkritische personenbezogene Daten und sensible personenbezogene Daten. Diese Kategorien haben Einfluss auf die Übersicht der eingeschalteten Unterauftragsverarbeiter und werden dort verwendet.

Kategorien personenbezogener Daten	**Systemkritische**	**Sensible personenbezogene Daten**
	Benutzer-ID	Name
	E-Mail	Geburtsdatum
	Benutzername + Passwort	Geschlecht
	IP-Adresse	Profilfoto (optional)
	Beschwerde- und Verbesserungsdaten	Telefon (optional)
	Gerätetyp	Funktionsbezeichnung
		Ausbildungsgeschichte
		Kompetenzen
		Entwicklungsdaten
		Zertifizierungen
		Beurteilungsdaten
		Ausgefüllte Fragenlisten
		Gesprächsnotizen

		Gehaltsdaten

Zwecke, für welche die personenbezogenen Daten verarbeitet werden

- Anlegen der Unternehmensumgebung
- Einrichtung der Unternehmensumgebung und Digitalisierung von HR-/Geschäftsprozessen
- Unterstützung und Durchführung von HR-/Geschäftsprozessen
- Beschwerde- und Vorfallbearbeitung

Der Kunde sichert zu, dass die in dieser Übersicht beschriebenen personenbezogenen Daten und Kategorien von Betroffenen vollständig und korrekt sind, und stellt Learned von jeglichen Mängeln und Ansprüchen frei, die sich aus einer inkorrekten Darstellung durch den Kunden ergeben.

Anhang 1b | Übersicht Unterauftragsverarbeiter

Learned ist berechtigt, bei der Durchführung des SaaS-Vertrags die nachstehenden Unterauftragsverarbeiter einzuschalten:

Name	Zweck des Unterauftragsverarbeiters	Art der personenbezogenen Daten	Kategorie der personenbezogenen Daten	Region/Land
Google Cloud Platform	Der Server des Plattform.	Alle	Beide	Frankfurt …
MongoDB	Die Datenbank des Plattform.	Alle	Beide	Frankfurt …
PostHog	Produktanalysen	IP-Adress…	Systemkri…	Frankfurt …
Hubspot	E-Mail-Software. Integrierter Chat und Helpdesk in der Plattform.	Name, E-…	Systemkri…	Frankfurt,…
Sentry	Performance- und Incident-Monitoring-Software	Benutzer-…	Systemkri…	Frankfurt,…

Auth0	Authentifizierungsplattform. Wird für sicheres Anmelden und Multi-Faktor-Authentifizierung verwendet.	Name, Be…	Systemkri…	Frankfurt …
OpenAI Ireland Limited	Bereitstellung von KI-Diensten	IP-Adress…	Beide	Frankfurt …
Mailgun	E-Mail-Server für den Versand von E-Mails (Benachrichtigungen).	Name, E-…	Systemkri…	Frankfurt,…
Kombo Technologies GmbH	Integrationsplattform (Unified API) für Anbindungen an HRIS-, ATS- und Gehaltsabrechnungssysteme des Kunden.	Benutzer-IDs, Name, E-Mail, Funktionsbezeichnung, Gehaltsdaten	Beide	Niederlande (Google Cloud, EU)