wowiconsult GmbH

API-Nutzungsbedingungen

Stand: 01.04.2026
Version: v1.0

API-Nutzungsbedingungen

zwischen

wowiconsult GmbH – nachfolgend „Auftragnehmerin" –

und dem jeweiligen Kunden – nachfolgend „Auftraggeber" –

Vorbemerkung

Diese API-Nutzungsbedingungen ergänzen die AGB und den SaaS-Vertrag der Auftragnehmerin. Sie gelten, soweit dem Auftraggeber der Zugriff auf Programmierschnittstellen (APIs) der Auftragnehmerin eingeräumt wird.

Soweit diese API-Nutzungsbedingungen abweichende Regelungen zu API-Zugriffen, API-Schlüsseln, Nutzungslimits, technischen Änderungen, Versionen, Sicherheitsanforderungen oder Sperrrechten enthalten, gehen sie den allgemeinen Regelungen des SaaS-Vertrags und der AGB insoweit vor.

§ 1 Anwendungsbereich

Diese API-Nutzungsbedingungen gelten für alle bereitgestellten APIs, Endpunkte, Entwicklerzugänge, Sandboxes, API-Schlüssel, Tokens, Webhooks und sonstigen technischen Schnittstellen der Auftragnehmerin, soweit nicht im Angebot oder in einer gesonderten Vereinbarung etwas Abweichendes geregelt ist.

Die API-Nutzung ist nur im Rahmen eines bestehenden Vertragsverhältnisses mit der Auftragnehmerin zulässig.

§ 2 API-Zugriffsrecht

Die Auftragnehmerin räumt dem Auftraggeber für die Vertragslaufzeit ein einfaches, nicht ausschließliches, nicht übertragbares und nicht unterlizenzierbares Recht ein, die vereinbarten APIs für eigene interne Geschäftszwecke im vertraglich vorgesehenen Umfang zu nutzen.

Eine Nutzung zur Bereitstellung eigenständiger Drittangebote, als Plattform für unberechtigte Dritte oder im Wege eines Reselling ist nur zulässig, wenn dies ausdrücklich in Textform vereinbart wurde.

§ 3 Dokumentation und technische Vorgaben

Die Nutzung der APIs setzt die Einhaltung der jeweils aktuellen technischen Dokumentation, Authentifizierungsverfahren, Integrationsvorgaben, Sicherheitsanforderungen und sonstigen technischen Rahmenbedingungen voraus.

Die Auftragnehmerin ist berechtigt, die Dokumentation und technischen Spezifikationen sachgerecht weiterzuentwickeln, soweit dies dem Auftraggeber zumutbar ist.

§ 4 API-Schlüssel und Zugangsdaten

API-Schlüssel, Tokens, Zugangsdaten und sonstige Authentifizierungsmerkmale sind vertraulich zu behandeln und vor dem Zugriff unbefugter Dritter zu schützen.

Der Auftraggeber haftet für alle Handlungen, die unter Verwendung seiner API-Schlüssel oder Zugangsdaten vorgenommen werden, soweit er den Missbrauch zu vertreten hat.

Der Auftraggeber informiert die Auftragnehmerin unverzüglich über den Verdacht eines Verlusts, Missbrauchs oder unbefugten Zugriffs.

§ 5 Nutzungsgrenzen und Fair Use

Die Auftragnehmerin ist berechtigt, im Angebot, in der Leistungsbeschreibung, in der Dokumentation oder technisch Rate Limits, Request-Limits, Bandbreitenbegrenzungen, Volumenobergrenzen oder sonstige Nutzungsgrenzen festzulegen.

Der Auftraggeber unterlässt jede Nutzung, die die Stabilität, Sicherheit oder Verfügbarkeit der API oder der damit verbundenen Systeme beeinträchtigen kann.

Bei Überschreitung vereinbarter oder technisch vorgegebener Nutzungsgrenzen ist die Auftragnehmerin berechtigt, Zugriffe zu drosseln, vorübergehend zu sperren oder Mehrnutzung gesondert abzurechnen.

§ 6 Unzulässige Nutzung

Unzulässig sind insbesondere:

- die Umgehung technischer Schutzmaßnahmen, Sicherheitsmechanismen oder Zugriffsbeschränkungen,
- Reverse Engineering, Dekompilierung oder sonstige Rückerschließung, soweit nicht zwingend gesetzlich zulässig,
- Scraping, Massenabfragen oder automatisierte Nutzungen außerhalb der vereinbarten Zweckbestimmung,
- die Nutzung zur Entwicklung konkurrierender Produkte oder zur Wettbewerbsanalyse,
- die Weitergabe von API-Zugängen an unberechtigte Dritte,
- die Einbindung in rechtswidrige, sicherheitsgefährdende oder technisch missbräuchliche Prozesse.

§ 7 Änderungen, Versionierung und Deprecation

Die Auftragnehmerin ist berechtigt, APIs, Endpunkte, Datenformate, Authentifizierungsverfahren und sonstige technische Komponenten weiterzuentwickeln, zu ändern oder durch neue Versionen zu ersetzen, soweit dies aus technischen, sicherheitsbezogenen, rechtlichen oder betrieblichen Gründen erforderlich ist.

Soweit zumutbar, wird die Auftragnehmerin den Auftraggeber über wesentliche Änderungen mit angemessener Vorlaufzeit informieren.

Veraltete oder abgekündigte API-Versionen können nach Ablauf einer angemessenen Übergangsfrist eingestellt werden.

Der Auftraggeber ist verpflichtet, erforderliche Anpassungen seiner Systeme innerhalb der mitgeteilten Fristen eigenverantwortlich vorzunehmen.

§ 8 Verfügbarkeit und Support

Die Verfügbarkeit, Servicezeiten, Reaktionszeiten und Wiederherstellungszeiten für API-bezogene Leistungen richten sich nach dem vereinbarten SLA, soweit die API dort oder im Angebot mit umfasst ist.

Soweit keine ausdrückliche Einbeziehung in das SLA vereinbart ist, schuldet die Auftragnehmerin für APIs nur den allgemeinen vertraglich vereinbarten Support.

§ 9 Datenverarbeitung und Datenschutz

Soweit über die APIs personenbezogene Daten verarbeitet werden, gelten ergänzend die datenschutzrechtlichen Vereinbarungen der Parteien, insbesondere eine gesonderte Auftragsverarbeitungsvereinbarung, soweit rechtlich erforderlich.

Der Auftraggeber bleibt für die Rechtmäßigkeit der über die APIs veranlassten Datenverarbeitungen, Abrufe und Übermittlungen verantwortlich, soweit diese aus seiner Sphäre stammen.

§ 10 Sicherheit und Incident Management

Der Auftraggeber hat seine Systeme, Integrationen und Zugangsdaten nach dem Stand der Technik angemessen abzusichern.

Bei Sicherheitsvorfällen, Missbrauchsverdacht, ungewöhnlichen Zugriffsmustern oder sonstigen Gefährdungen ist die Auftragnehmerin berechtigt, API-Zugänge vorübergehend ganz oder teilweise zu sperren, einzuschränken, Schlüssel zurückzusetzen oder andere geeignete Schutzmaßnahmen zu ergreifen.

Die Auftragnehmerin wird den Auftraggeber über solche Maßnahmen so bald wie angemessen informieren, soweit dem keine sicherheitsrelevanten Gründe entgegenstehen.

§ 11 Audit, Nachweise und technische Prüfungen

Individuelle Audits, Penetrationstests, Lasttests oder sonstige technische Prüfungen der APIs durch den Auftraggeber oder durch von ihm beauftragte Dritte bedürfen der vorherigen Zustimmung der Auftragnehmerin in Textform.

Unangekündigte oder nicht abgestimmte technische Prüfungen sind unzulässig.

§ 12 Rechtsfolgen bei Verstößen

Bei Verstößen gegen diese API-Nutzungsbedingungen ist die Auftragnehmerin berechtigt, nach pflichtgemäßem Ermessen einzelne API-Zugänge zu sperren, die Nutzung einzuschränken, Schlüssel zu deaktivieren oder den Zugriff insgesamt zu unterbinden, sofern und soweit dies zur Abwehr von Risiken, zur Aufrechterhaltung des Betriebs oder zur Durchsetzung der vertraglichen Regelungen erforderlich ist.

Weitergehende Rechte, insbesondere Vergütungsansprüche, Unterlassungsansprüche, Schadensersatzansprüche und Kündigungsrechte, bleiben unberührt.

§ 13 Rangfolge

Individuelle Vereinbarungen, Angebote und Leistungsbeschreibungen gehen diesen API-Nutzungsbedingungen vor.

Der SaaS-Vertrag geht diesen API-Nutzungsbedingungen vor, soweit er speziellere Regelungen zu Vergütung, Laufzeit, Vertragsbeendigung oder Hauptleistungspflichten enthält.

Diese API-Nutzungsbedingungen gehen dem SaaS-Vertrag und den AGB insoweit vor, als sie speziellere Regelungen zur API-Nutzung, zu Zugängen, technischen Änderungen, Nutzungsgrenzen, Sicherheitsmaßnahmen oder Sperrrechten enthalten.

Im Übrigen gelten die AGB der Auftragnehmerin ergänzend.

§ 14 Schlussbestimmungen

Änderungen und Ergänzungen dieser API-Nutzungsbedingungen bedürfen der Textform, soweit nicht gesetzlich eine strengere Form erforderlich ist.