

CHECKLISTE ZU KI FÜR VERTRÄGE MIT LIEFERANTEN UND PARTNERN

David Rosenthal


Projekt/Anbieter: Bewertet:

Anforderung (★ = Grundschatz)	Datenschutz	Geheimnispflichten	Urheberrecht	KI-Regulierung	Allgemein	Bewertung des Projekts/Anbieters
Identifizierung von KI Es wurde festgelegt, wo der Lieferant oder Partner in seinen Dienstleistungen, Produkten oder Aktivitäten künstliche Intelligenz (KI) verwendet, und er ist verpflichtet, eine solche Verwendung offenzulegen, sobald sie stattfindet. Unter KI kann jedes automatisierte System verstanden werden, das zu einem gewissen Grad autonom arbeitet (d.h. das nicht nur programmiert, sondern auch "trainiert" worden ist).				✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Auftragsverarbeitungsvereinbarung ★ Wo der Lieferant oder Partner Auftragsverarbeiter ist, ist mit ihm eine Vereinbarung zur Auftragsverarbeitung abgeschlossen, welche den Anforderungen des geltenden Datenschutzrechts, so namentlich der DSGVO und dem Schweizer DSG, entspricht.	✓					<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Data Sharing/Joint Controller Agreement Wo der Lieferant oder Partner alleiniger oder gemeinsamer Verantwortlicher ist, wurden die Verantwortlichkeiten des Lieferanten und Partners sowie des Kunden festgelegt, einschliesslich etwaiger Zusicherungen in Bezug auf gemeinsam genutzte oder erhobene (personenbezogene) Daten sowie Einschränkungen bei der Verarbeitung dieser Daten durch eine der Parteien.	✓	✓			✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Beschränkung der Datennutzung durch den Anbieter ★ Das Recht des Lieferanten oder Partners, Daten des Kunden und andere Daten, die der Kunde im Rahmen mit den Dienstleistungen, Produkten und Aktivitäten erhebt, für das Training von eigenen KI-Modellen und andere Sekundärnutzungen zu verwenden, wurde ausdrücklich ausgeschlossen oder speziell geregelt, dies in Übereinstimmung mit dem, was der Kunde bereit ist zu erlauben und erlauben darf. In der Regel sollte kein KI-Training oder eine andere Sekundärnutzung erlaubt sein, es sei denn, dies ist für die Dienstleistungen, Produkte oder Aktivitäten erforderlich. Erfolgt ein KI-Training oder eine sonstige Sekundärnutzung nur auf "anonymisierter" Basis, sollten die Standards für die Anonymisierung und die Validierung ihrer Wirksamkeit vereinbart werden. Für den Fall, dass Daten für Trainingszwecke	✓	✓	✓			<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A

VISCHER

verwendet werden, sollte der Schutz vor "Datenlecks" in den daraus resultierenden KI-Modellen und die Einhaltung der Rechte der betroffenen Personen (einschliesslich des Widerrufs der Einwilligung, wo relevant ist) geregelt werden.						
Verpflichtung zur Löschung Nach Beendigung des Vertragsverhältnisses lässt der Lieferant oder Partner die Daten des Kunden, auch wenn sie nicht personenbezogen sind, endgültig und ohne Rückbehalt einer Kopie löschen, es sei denn, er wäre zur Aufbewahrung gesetzlich verpflichtet oder eine Löschung ist vernünftigerweise nicht möglich (z.B. bei Backups); in diesem Fall müssen die Daten weiterhin vertraulich behandelt werden.	✓	✓	✓			<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Grenzüberschreitende Übermittlung ist abgesichert ★ Jegliche Übermittlung personenbezogener Daten (auch durch Fernzugriff) an den Lieferanten oder Partner oder an dessen Unterauftragnehmer oder andere beteiligte Dritte stehen im Einklang mit den Vorgaben für grenzüberschreitende Übermittlungen solcher Daten, d.h., personenbezogene Daten dürfen nur in Länder mit einem entsprechenden Angemessenheitsbeschluss oder mit vertraglichen Garantien (z.B. EU SCC, ggf. mit länderspezifischen Anpassungen) übermittelt werden. Nötigenfalls ist ein Transfer Impact Assessment mit positivem Ergebnis durchgeführt worden.	✓					<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Kein Verkauf von Daten an Dritte ★ Die Daten des Kunden und andere Daten, die der Lieferant oder der Partner auf Seiten des Kunden im Zusammenhang mit den Dienstleistungen, Produkten und Aktivitäten erhoben hat, werden nicht an Dritte verkauft oder diesen anderweitig zur Verfügung gestellt, es sei denn, dies wurde im Einzelfall ausdrücklich mit dem Kunden vereinbart.	✓	✓	✓			<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Angemessene Informationssicherheit ★ Der Lieferant bzw. Partner verpflichtet sich, technische und organisatorische Massnahmen vorzusehen, die ein angemessenes Niveau an Informationssicherheit in Bezug auf seine Dienstleistungen, Produkte und Aktivitäten gewährleisten. Sie berücksichtigen die spezifischen Mittel, mit denen KI-Systeme angegriffen werden können, z.B. durch Prompt Injections/Jailbreaking, Poisoning und Sponge-Angriffe.	✓	✓	✓	✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Rechte der betroffenen Personen Die Parteien haben sich darauf geeinigt, wie mit berechtigten Anfragen von Personen umzugehen ist, die von der Verarbeitung ihrer personenbezogenen Daten oder sonst dem Einsatz von KI betroffen sind (auch wenn keine personenbezogenen Daten betroffen sind). Dazu kann gehören, dass der Lieferant oder Anbieter verpflichtet wird, in Verbindung mit seinen Dienstleistungen, Produkten und Aktivitäten bestimmte Funktionen bereitzustellen, die es dem Kunden ermöglichen, die Daten dieser Personen zu löschen, zu sperren oder zu suchen und auf sie zuzugreifen (z.B. Filterung von KI-Inputs und -Outputs in Bezug auf das Vorkommen bestimmter personenbezogener Daten oder Inhalte Dritter).	✓		✓	✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A

VISCHER

<p>Vertraulichkeitsverpflichtung </p> <p>Der Lieferant oder Partner wird selbst und durch schriftliche Erklärungen seine Mitarbeitenden und Unterauftragnehmer zur Geheimhaltung von Kundendaten verpflichten und diese mit technischen und organisatorischen Mitteln der Informationssicherheit schützen, die der Sensibilität der Daten und dem Risiko ihrer Verarbeitung angemessen sind. Soweit es sich um ein Berufs- oder Amtsgeheimnis handelt, ist hierauf ausdrücklich hinzuweisen. Die Verpflichtung zur Geheimhaltung der Daten besteht so lange, wie es das geltende Recht erfordert oder ein berechtigtes Interesse des Kunden (oder betroffener Dritter) an der Geheimhaltung der Daten besteht. Im Rahmen der Geheimhaltungsverpflichtung sollte sich der Lieferant oder Partner auch verpflichten, die Kundendaten nicht für andere Zwecke als die Vertragserfüllung zu verwenden.</p>		✓	✓			<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>"Defend-your-data"-Klausel</p> <p>Der Lieferant oder Partner wird, wenn er mit dem Versuch einer Behörde oder eines sonstigen Dritten konfrontiert wird, auf die Daten des Kunden zuzugreifen oder deren Herausgabe zu verlangen, (i) den Kunden informieren und den Dritten an den Kunden verweisen (sofern zulässig) und (ii) sofern er vom Kunden nicht anderweitig angewiesen wird, in jedem Fall alle rechtlichen Mittel auszuschöpfen, um einem solchen Zugriff oder eine solche Herausgabe zu verhindern (auch mit der Begründung, dass sie gegen das Recht im Land des Kunden verstösst), oder, falls dies nicht möglich ist, den Umfang zu begrenzen und alle verfügbaren Schutzmassnahmen zur Anwendung zu bringen.</p>		✓				<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>Beschränkung des Zugriffs für das Personal des Lieferanten</p> <p>Das Personal des Lieferanten oder Partners (oder seiner Unterauftragnehmer) darf nur dann auf die Daten des Kunden zugreifen, wenn dies entweder vom Kunden in jedem Einzelfall genehmigt worden ist oder wenn dies für die Erfüllung einer vollstreckbaren, rechtsverbindlichen Anordnung (oder wegen geltendem Recht [des Kunden]) erforderlich ist. Ausnahmen können vereinbart werden für den Fall, dass die Dienstleistung, das Produkt oder die Aktivitäten ihrer Art nach den Zugriff auf Daten des Kunden durch das Personal des Lieferanten erfordern.</p>		✓				<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>Geo-Lokalisierung von Daten</p> <p>Der Anbieter oder Partner speichert [und verarbeitet] die Daten des Kunden ausschliesslich in den mit dem Kunden vereinbarten geografischen Regionen[, auch zum Zwecke des Kundensupports, der Sicherheitsmassnahmen und der Missbrauchskontrolle]. Diese Geo-Lokalisierung ist möglicherweise nur für bestimmte Dienstleistungen verfügbar.</p>	✓	✓				<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>KI-Regulierung wird befolgt</p> <p>Die Dienstleistungen, Produkte oder Aktivitäten des Lieferanten oder Partners müssen der für den Anbieter oder Partner und den Kunden geltenden KI-Regulierung entsprechen, einschliesslich des EU AI Act (soweit anwendbar). Dazu gehört auch, dass die jeweiligen regulatorischen "Rollen" des</p>				✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A

VISCHER

Lieferanten oder Partners und des Kunden (Anbieter, Einführer, Betreiber usw.) festgelegt und vereinbart wurden.						
Unterstützung bei der Befolgung der KI-Regulierung Der Lieferant oder Partner wird dem Kunden jede vernünftigerweise von ihm verlangte Unterstützung gewähren, die er benötigt, um seinerseits die auf ihn anwendbaren Vorschriften der KI-Regulierung einzuhalten, einschliesslich durch das Bereitstellen der erforderlichen Unterlagen und das Beantworten von Fragen.				✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Keine verbotenen KI-Praktiken Die Dienstleistungen, Produkte oder Aktivitäten des Lieferanten oder Partners stellen bei bestimmungsgemässer Nutzung keine verbotenen Praktiken gemäss der auf den Lieferanten und Partner wie auch auf den Kunden anwendbaren KI-Regulierung dar.				✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Verwendung von Wasserzeichen Die Parteien haben vereinbart, ob und wie die durch die Dienstleistungen, Produkte oder Aktivitäten des Lieferanten oder Partners erzeugten Inhalte mit Wasserzeichen oder anderen Markierungen gemäss den gesetzlichen Vorgaben versehen sein werden, so insbesondere wenn sie mittels KI erzeugt oder verändert worden sind.			✓	✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Überwachung, Meldung von Zwischenfällen Der Lieferant oder Partner beobachtet laufend seine Dienstleistungen, Produkte und Aktivitäten auf etwaige Zwischenfälle hin (auch solche, die bei anderen Kunden Benutzern geschehen), und meldet dem Kunden alle Entwicklungen, die auf ein problematisches KI-Verhalten oder eine problematische KI-Nutzung hindeuten oder anderweitig im Hinblick auf die Zuverlässigkeit, Sicherheit und Konformität seiner Dienstleistungen, Produkte und Aktivitäten relevant sein könnten.				✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
De-Biasing Der Lieferant oder Partner muss die KI-Modelle, die er für seine Dienstleistungen, Produkte und Aktivitäten verwendet, angemessen trainieren, abstimmen (Fine Tuning) oder sonst so kontrollieren, dass die damit erzeugten Ergebnisse keine unerwünschten Verzerrungen (Bias) aufweisen. Er hat diese Dienstleistungen, Produkte und Aktivitäten daraufhin getestet.	✓			✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Audit-Trails / Protokollierung Der Lieferant oder Partner muss es dem Kunden ermöglichen, die Eingaben, die Ausgaben und die sonstige Nutzung seiner Dienstleistungen, Produkte oder Aktivitäten in Form von Protokollen vollständig zu dokumentieren. Diese Protokolle müssen unveränderbar sein und pro Benutzer erfolgen. Der Kunde muss die Möglichkeit haben, sie mindestens ein Jahr lang aufzubewahren.	✓			✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A

VISCHER

<p>Rechtskonformes KI-Modell-Training</p> <p>Der Anbieter oder Partner verpflichtet sich und gewährleistet, dass die KI-Modelle, die von seinen Dienstleistungen, Produkten und Aktivitäten verwendet werden, in Übereinstimmung mit geltendem Recht trainiert worden sind, wobei dieses Recht auch das auf den Kunden anwendbare Recht, die von den Parteien sonst bezeichneten Rechtsordnungen und im Falle von Allzweck-KI-Modellen unter dem EU AI Act auch das EU-Urheberrecht umfassen. Umfassen die Dienstleistungen, Produkte und Aktivitäten das Training oder Feinabstimmen von KI-Modellen, so gelten diese Verpflichtungen entsprechend.</p>	✓		✓	✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>Gebrauchsanweisung und Support</p> <p>Der Lieferant oder Partner stellt dem Kunden angemessene Anweisungen, Schulungen und Unterstützung zur Verfügung, wie die von ihm gelieferten Dienstleistungen oder Produkte bzw. die von ihm durchgeführten Aktivitäten ordnungsgemäss zu nutzen sind und wie mit eventuell auftretenden Problemen umzugehen ist. In diesen Anweisungen sind auch alle bekannten Probleme und Risiken anzugeben, die angemessen berücksichtigt werden müssen.</p>			✓	✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>Getestete KI</p> <p>Der Lieferant oder Partner verpflichtet sich und gewährleistet, dass er die Dienstleistungen, Produkte und Aktivitäten vor der Freigabe zur produktiven Nutzung angemessen auf die Erfüllung der Anforderungen geprüft hat bzw. prüfen wird. Diese Prüfungen sind zu dokumentieren, wobei die Dokumentation dem Kunden zur Verfügung zu stellen ist.</p>	✓		✓	✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>Erklärbarkeit</p> <p>Der Lieferant oder Partner stellt dem Kunden die erforderlichen Unterlagen und sonstigen Informationen zur Verfügung, damit der Kunde in angemessener Weise nachvollziehen kann, (i) wie die KI-Komponenten, die in oder von den Dienstleistungen, Produkten und Aktivitäten verwendet werden, funktionieren und (ii) warum die KI grundsätzlich den Output erzeugt wie sie es tut oder die Entscheidung trifft, wie sie sie trifft (was ein Verständnis der grundlegenden Logik der KI und der Daten, auf die sie sich bei ihrer Anwendung stützt, erfordert).</p>	✓		✓	✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>Menschliche Aufsicht</p> <p>Der Lieferant oder Partner verpflichtet sich und gewährleistet, dass die KI-Komponenten seiner Dienstleistungen und Produkte über die erforderlichen Funktionen verfügen, die es dem Kunden ermöglichen, die Kontrolle zu behalten. Wenn der Anbieter oder Partner selbst KI für seine Aktivitäten einsetzt, verpflichtet er sich, jede Nutzung von KI, die relevante negative Folgen für Dritte (einschliesslich den Kunden) haben könnte, selbst durch Menschen überwachen und diese nötigenfalls eingreifen zu lassen.</p>	✓		✓	✓		<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
<p>IP-Schadloshaltung</p> <p>Der Lieferant oder Partner verteidigt, hält den Kunden schad- und klaglos für den Fall, dass ein Dritter behauptet, dass die durch die Dienstleistungen, Produkte oder Aktivitäten des Lieferanten oder Partners erzeugten Ergebnisse</p>			✓			<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A

VISCHER

seine IP-Rechte verletzen. Wo Einschränkungen und Begrenzungen für eine solche IP-Schadloshaltung gelten, wurden diese festgelegt und sind akzeptabel.						
Guardrails Der Anbieter oder Partner muss sog. Guardrails und andere Funktionen vorsehen, die den KI-Input und -Output seiner Dienstleistungen, Produkte und Aktivitäten begrenzen im Hinblick auf bestimmtes problematisches Verhalten oder problematische Ergebnisse, wie verbotene oder unethische Nutzung, illegale Inhalte oder Verletzung von Rechten Dritter. Dazu kann auch das Filtern oder Sperren bestimmter personenbezogener Daten oder Inhalte gehören, wenn betroffene Personen oder Rechteinhaber dies verlangen.	✓		✓		✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Zuverlässigkeit Der Lieferant oder Partner muss seine Dienstleistungen, Produkte und Aktivitäten so entwickeln und durchführen lassen, dass ihr KI-Output von angemessener Zuverlässigkeit ist, so insbesondere im Hinblick auf seine Richtigkeit und Vollständigkeit für den jeweiligen Zweck. Es sind Massnahmen vorgesehen, um Ergebnisse für die Zukunft zu korrigieren, sollte sich der bestehende Grad an Zuverlässigkeit als unzureichend erweisen.				✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Missbrauchsüberwachung Es wurde vereinbart, dass nur der Lieferant oder Partner, nur der Kunde oder beide die Dienstleistungen, die Nutzung der Produkte oder die Aktivitäten auf mögliche missbräuchliche Nutzung durch ihre Nutzer überwachen werden oder sollen.		✓			✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Recht auf Nutzung des Outputs ★ Die Parteien haben vereinbart, in welchem Umfang der Kunde (einschliesslich seiner Nutzer) den durch die Dienstleistungen, Produkte oder Aktivitäten erzeugten Output nutzen darf, einschliesslich der Frage, ob er nur für bestimmte Zwecke oder unter anderen Beschränkungen genutzt werden darf, wer Eigentümer des Outputs ist und ob gegebenenfalls zusätzliche Zahlungen zu leisten sind.			✓			<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Qualität des Trainings der KI-Modelle Die Parteien haben die erforderliche Qualität und anderen Eigenschaften der zu verwendenden KI-Modelle (einschliesslich ihres Trainings, ihrer Prüfung und Validierung) sowie die Art und Weise, wie diese Aspekte dokumentiert, gemessen und überprüft werden sollen, und die Massnahmen für den Fall, dass die Vorgaben nicht eingehalten sind. Umfassen die Dienstleistungen, Produkte und Aktivitäten Trainings oder Feinabstimmungen, so gelten diese Verpflichtungen entsprechend.					✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Nutzungsrichtlinien ★ Die Parteien haben vereinbart, welche Einschränkungen in Bezug auf die Nutzung der Dienstleistungen, Produkte und Aktivitäten durch den Kunden (und seine Nutzer) gelten, z.B. dass bestimmte Kategorien von Inhalten nicht erstellt werden dürfen oder bestimmte Nutzungszwecke nicht zulässig sind.			✓		✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Vertragsänderungen Die Parteien haben vereinbart, wie und unter				✓	✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK

VISCHER

welchen Bedingungen (i) die Vertragsbedingungen einseitig geändert werden können, z.B. durch neue Leistungsbedingungen seitens des Lieferanten oder Partners, und (ii) wie neue rechtliche und regulatorische Anforderungen, die eine Vertragsänderung vernünftigerweise erfordern, umgesetzt werden (z.B. Pflicht zur Verhandlung einer Änderung).						<input type="checkbox"/> N/A
Haftung/Schadloshaltung Der Lieferant oder Partner schränkt die Haftung im Hinblick auf bekannte und unbekannte Risiken von KI nicht unangemessen ein und schliesst sie nicht in unangemessener Weise aus. Er sorgt für eine angemessene Entschädigung für den Fall, dass seine Vertrags- oder Rechtsverletzung zu Ansprüchen Dritter gegen den Kunden führt.					✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A
Abbildemassnahmen im Falle von Vertragsverletzungen Die Parteien haben die dem Kunden zur Verfügung stehenden Rechtsbehelfe und sonstigen Folgen für den Fall vereinbart, dass der Lieferant oder Partner die vereinbarten Verpflichtungen und übernommenen Gewährleistungen nicht einhält.					✓	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> N/A

Hinweis: Diese Checkliste dient nur zu Informationszwecken und stellt keine Rechtsberatung dar. Sie ist auf europäische Unternehmen ausgerichtet. Wenn Sie Fehler entdecken oder glauben, dass etwas fehlt, lassen Sie es uns wissen unter ai@vischer.com. Die neueste Version finden Sie unter <https://vischerlnk.com/ki-provider-check>. Sie ist auch in englischer Sprache verfügbar (<https://vischerlnk.com/ai-provider-check>). Weitere Informationen über künstliche Intelligenz finden Sie unter <https://vischer.com/ai>, einschliesslich eines Blog-Beitrags (Nr. 15), der weitere Informationen zur oben genannten Checkliste enthält.