Datenschutzvereinbarung nach Art. 28 DSGVO

Verarbeitung personenbezogener Daten im Auftrag

---

zwischen

lector.ai GmbH
Konsul-Smidt-Straße 8p
28217 Bremen
- nachfolgend “lector.ai” genannt -

und

{{CUSTOMER_NAME}}
{{CUSTOMER_STREET}}
{{CUSTOMER_POSTAL_CODE}} {{CUSTOMER_CITY}}
{{CUSTOMER_COUNTRY}}
- nachfolgend “Kunde” genannt -

Stand: 29. Juli 2025

Präambel

Der Kunde nutzt den von lector.ai betriebenen internetbasierten Dienst zur Verarbeitung von Dokumenten. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Kunde personenbezogene Daten verarbeitet. Nach Art. 28 DSGVO ist hierfür der Abschluss eines Auftragsverarbeitungsvertrags erforderlich.

Voraussetzung für die Zulässigkeit einer solchen Auftragsverarbeitung i. S. d. Art. 28 DSGVO ist, dass der Kunde lector.ai den Auftrag erteilt. Dieser Vertrag enthält diesen Auftrag des Kunden an lector.ai und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Datenverarbeitung sowie die sich daraus ergebenden besonderen Pflichten in Bezug auf Datenschutz und Datensicherheit.

Grundsätzlich ist der Kunde für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz verantwortlich und behält insofern die Herrschaft über die zu verarbeitenden Daten. lector.ai wird den Kunden hierbei in geeigneter Weise unterstützen.

1. Gegenstand, Umfang und Dauer des Auftrags

1.1 Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem zugrunde liegenden Auftrag in Zusammenhang stehen und bei denen Mitarbeiter von lector.ai oder durch lector.ai beauftragte Dritte mit personenbezogenen Daten des Kunden in Berührung kommen können. Der Auftrag des Kunden an lector.ai umfasst die in der **Anlage 1** wiedergegebenen Arbeiten und/oder Leistungen. Aus der Anlage ergibt sich zudem der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen.

1.2 Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über Nutzung der Dienstleistungen von lector.ai durch den Kunden. Das Recht zur außerordentlichen Kündigung bei Vorliegen eines wichtigen Grundes bleibt unberührt. Ein wichtiger Grund in diesem Sinne ist insbesondere dann gegeben, wenn lector.ai gegen Bestimmungen der DSGVO oder gegen Bestimmungen dieses Auftragsverarbeitungsvertrages verstößt.

1.3 Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie lector.ai personenbezogene Daten des Kundes verarbeitet (einschließlich Backups).

1.4 Soweit sich aus anderen Vereinbarungen zwischen dem Kunden und lector.ai anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Rechte betroffener Personen

2.1 Der Kunde ist für die Wahrung der Betroffenenrechte allein verantwortlich. lector.ai ist verpflichtet, den Kunden bei seiner Pflicht, Betroffenenanfragen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. lector.ai hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Kunden erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

2.2 Soweit eine Mitwirkung von lector.ai für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Kunden erforderlich ist, wird lector.ai die jeweils erforderlichen Maßnahmen nach Weisung des Kunden treffen. lector.ai wird den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

3. Rechte und Pflichten sowie Weisungsbefugnis des Kunden

3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO ist allein der Kunde verantwortlich.

3.2 Der Kunde ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch lector.ai. lector.ai steht nach Ziff. 4 c) das Recht zu, den Kunden darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

3.3 Der Kunde ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. lector.ai wird den Kunden unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber lector.ai geltend machen.

3.4 Der Kunde hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber lector.ai zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

3.5 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Kunden bei lector.ai entstehen, bleiben unberührt.

3.6 Der Kunde informiert lector.ai unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3.7 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Kunden geltenden gesetzlichen Meldepflicht besteht, ist der Kunde für deren Einhaltung verantwortlich.

4. Kontrollbefugnisse des Kunden

4.1 Der Kunde hat das Recht, in Zusammenarbeit mit lector.ai unentgeltlich Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung und insbesondere der in **Anlage 2** festgelegten technischen und organisatorischen Maßnahmen durch lector.ai in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

4.2 lector.ai ist dem Kunden gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes (1) erforderlich ist.

4.3 lector.ai stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten von lector.ai nach Art. 28 DSGVO überzeugen kann. Der Kunde kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. (1) in der Betriebsstätte von lector.ai zu den jeweils üblichen Geschäftszeiten vornehmen. Der Kunde wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe von lector.ai durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Kunden unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen werden der Kunde und lector.ai die

entstehenden Aufwände für die Betreuung und Begleitung der Kontrollpersonen vor Ort gesondert vereinbaren.

4.4 Weitere Nachweise solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, können erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

5. Pflichten von lector.ai

5.1 lector.ai verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder dessen Mitgliedstaaten, dem lector.ai unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt lector.ai dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Kunden. Eine hiervon abweichende Verarbeitung von Daten ist lector.ai untersagt, es sei denn, dass der Kunde dieser schriftlich zugestimmt hat.

5.3 lector.ai verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Kunden nicht erstellt.

5.4 lector.ai sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. lector.ai sichert zu, dass die für den Kunden verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

6.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Kunden ist lector.ai nur mit Genehmigung des Kunden gestattet, welche schriftlich oder in einem elektronischen Format erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn lector.ai dem Kunden Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss lector.ai dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

6.2 lector.ai ist berechtigt, die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang einzusetzen. Mit deren Beauftragung erklärt sich der Kunde einverstanden.

6.3 lector.ai hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen dem Kunden und lector.ai getroffenen Vereinbarungen einhalten kann. lector.ai hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. lector.ai wird den Kunden im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 2 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform zu informieren. Der Kunde hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen 2 Wochen nach Zugang der Information zu widersprechen. Der Widerspruch kann vom Kunden jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs wird lector.ai nach eigenem Ermessen entweder:

1. auf den Einsatz des geplanten Unterauftragnehmers verzichten und, soweit möglich und wirtschaftlich zumutbar, eine alternative Lösung anbieten; oder

2. wenn ein Verzicht auf den Unterauftragnehmer für lector.ai nicht möglich ist, besteht für beide Vertragsparteien ein Sonderkündigungsrecht mit einer Frist von 14 Tagen zum Ende eines Kalendermonats. Dieses Sonderkündigungsrecht kann innerhalb von 14 Tagen nach Mitteilung von lector.ai, dass ein Verzicht auf den Unterauftragnehmer nicht möglich ist, ausgeübt werden.

Wenn kein Widerspruch des Kunden binnen zwei Wochen nach Zugang der Information erfolgt, gilt dies als Zustimmung des Kunden zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers. Auf die Bedeutung seines Schweigens wird der Kunde in der Information gesondert hingewiesen.

6.4 lector.ai hat die Einhaltung der Pflichten der Subunternehmer zu überprüfen, das Ergebnis der Überprüfungen zu dokumentieren und dem Kunde auf Verlangen zugänglich zu machen.

7. Sonstige Pflichten von lector.ai

7.1 lector.ai hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet lector.ai insbesondere die Einhaltung folgender Vorgaben:

7.1.1 Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Kontaktdaten:

Tel.: +49 421 40887928
E-Mail: <datenschutz@jaai-group.com>

Ein Wechsel des Datenschutzbeauftragten ist dem Kunden unverzüglich mitzuteilen.

7.1.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. lector.ai setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. lector.ai und jede lector.ai unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

7.1.3 Der Kunde und lector.ai arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

7.1.4 Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei lector.ai ermittelt.

7.1.5 Soweit der Kunde seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei lector.ai ausgesetzt ist, hat ihn lector.ai nach besten Kräften zu unterstützen.

7.1.6 lector.ai kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

7.1.7 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden im Rahmen seiner Kontrollbefugnisse nach Ziffer 4 dieses Vertrages.

7.1.8 lector.ai unterstützt den Kunden in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung.

7.1.9 Soweit der Kunde zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn lector.ai unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

7.2 Dieser Vertrag entbindet lector.ai nicht von der Einhaltung anderer Vorgaben der DSGVO.

7.3 Kopien oder Duplikate der Daten werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

7.4 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Kunde – spätestens mit Beendigung des Hauptvertrags – hat lector.ai sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die

im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

7.5 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch lector.ai entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. lector.ai kann sie zu seiner Entlastung bei Vertragsende dem Kunden übergeben.

8. Technisch-organisatorische Maßnahmen

8.1 lector.ai hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Kunden zur Prüfung zu übergeben. Bei Akzeptanz durch den Kunden werden die dokumentierten Maßnahmen als **Anlage 2** Grundlage des Auftrages. Soweit eine Prüfung/ein Audit des Kunden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

8.2 lector.ai hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme von lector.ai. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

8.3 lector.ai ist verpflichtet, die in Anlage 2 vereinbarten Maßnahmen während der gesamten Vertragslaufzeit nach dem jeweiligen Stand der Technik durchzuführen.

8.4 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es lector.ai gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen muss lector.ai dem Kunden in dokumentierter Form (schriftlich, elektronisch) mitteilen.

9. Protokoll bei Datenschutzverletzungen

9.1 **Meldung von Datenschutzverletzungen:** lector.ai ist verpflichtet, den Kunden unverzüglich und, soweit möglich, spätestens 48 Stunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen. Die Meldung muss mindestens Folgendes enthalten:

9.1.1 Eine Beschreibung der Art der Datenschutzverletzung, einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl der betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen personenbezogenen Datensätze.

9.1.2 Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle, bei der weitere Informationen eingeholt werden können.

9.1.3 Eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung.

9.1.4 Eine Beschreibung der von lector.ai ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung, einschließlich, soweit zutreffend, Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

9.2 **Abmilderungsmaßnahmen:** lector.ai hat alle notwendigen und angemessenen Maßnahmen zu ergreifen, um die Auswirkungen der Datenschutzverletzung zu mildern und weitere Verletzungen zu verhindern.

9.3 **Dokumentation:** lector.ai hat alle Datenschutzverletzungen zu dokumentieren, einschließlich der damit zusammenhängenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss es dem Kunden ermöglichen, die Einhaltung dieser Klausel zu überprüfen.

10. Streitbeilegung

10.1 **Gütliche Einigung:** Im Falle eines Streits, der sich aus oder im Zusammenhang mit diesem Vertrag ergibt, werden die Parteien zunächst versuchen, den Streit gütlich durch Verhandlungen beizulegen.

10.2 **Mediation:** Kann der Streit nicht innerhalb von 30 Tagen durch Verhandlungen beigelegt werden, vereinbaren die Parteien, den Streit durch Mediation zu klären, bevor sie rechtliche Schritte einleiten. Die Mediation findet in Bremen, Deutschland, statt und die Sprache der Mediation ist Deutsch.

10.3 **Schiedsverfahren:** Wird der Streit nicht innerhalb von 60 Tagen nach Beginn der Mediation beigelegt, wird der Streit endgültig durch ein Schiedsverfahren gemäß den Regeln des Deutschen Instituts für Schiedsgerichtsbarkeit (DIS) entschieden. Das Schiedsverfahren findet in Bremen, Deutschland, statt und die Sprache des Schiedsverfahrens ist Deutsch.

10.4 **Kosten:** Jede Partei trägt ihre eigenen Kosten, die aus den Mediations- und Schiedsverfahren entstehen, es sei denn, die Parteien vereinbaren etwas anderes oder der Schiedsrichter entscheidet anders.

10.5 **Vertraulichkeit:** Alle Verhandlungen, Mediations- und Schiedsverfahren im Zusammenhang mit dem Streit sind vertraulich und dürfen ohne vorherige schriftliche Zustimmung der anderen Partei nicht an Dritte weitergegeben werden, es sei denn, dies ist gesetzlich vorgeschrieben.

11. Sonstige Bestimmungen

11.1 Auf alle aus diesem Vertrag oder im Zusammenhang damit entstehenden Rechtsfragen zwischen den Vertragspartnern findet ausschließlich die DSGVO in deutschsprachiger Fassung sowie im Übrigen das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts Anwendung.

11.2 Vorbehaltlich eines anderweitigen zwingenden Gerichtsstands ist ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder in Verbindung mit diesem Vertrag Bremen.

11.3 Sollten einzelne Bestimmungen dieses Vertrages inkl. seiner Anlagen unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. An die Stelle der unwirksamen Bestimmung setzen die Parteien einvernehmlich eine solche Ersatzregelung, die dem mit der unwirksamen Bestimmung angestrebten Zweck möglichst nahekommt. Entsprechendes gilt im Falle etwaiger Lücken im Vertrag.

Bremen, den 18.11.2025

Benjamin von Ardenne

Geschäftsführer lector.ai GmbH

Der Kunde hat seine Willenserklärung zum Abschluss des Vertrages elektronisch am 18.11.2025 durch den Nutzer mit der E-Mail Adresse abgegeben.

Anlage 1: Beschreibung der Datenverarbeitung von lector.ai

Stand: 29. Juli 2025

1 Umfang, Art und Zweck:

Verarbeitung von Dokumenten unterschiedlicher Kategorien; insbesondere Kategorisierung und Informations-Extraktion.

2 Arten von Daten:

Jegliche durch den Kunden im Dienst gespeicherte Daten, insbesondere von ihrer Endkundschaft, Lieferant:innen oder Mitarbeitenden, nämlich Name, Anschrift, E-Mail-Adressen, ggf. Telefonnummer, sowie Details zu getätigten Bestellungen.

3 Betroffene:

Endkundschaft, Lieferant:innen, Mitarbeitende.

Anlage 2: Checkliste technische und organisatorische Maßnahmen im Rahmen der Auftragsverarbeitung

Stand: 29. Juli 2025

Die nachfolgende Checkliste umfasst technische und organisatorische Maßnahmen, die im Rahmen der Auftragsverarbeitung umgesetzt werden können. Die Auswahl und Umsetzung der Maßnahmen erfolgt unter Berücksichtigung der spezifischen Anforderungen und Gegebenheiten des Auftraggebers und Auftragnehmers.

Kontakt Datenschutzbeauftragte:

Tel.: +49 421 40887928
E-Mail: <datenschutz@jaai-group.com>

Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen beziehen sich ausschließlich auf die Datenverarbeitung durch lector.ai und gelten nicht für externe Dienstleister, insbesondere Cloud-Dienstleister.

Bei der Beantwortung der Fragen wird in der Spalte “Erfüllt?” aus folgenden Werten gewählt:

- “Ja”, “Ja (gem. Zertifikat)” oder “Nein” entsprechend des aktuellen Umsetzungsstandes,
- “n/a”, wenn diese Maßnahme nicht zutrifft oder nicht sinnvoll ist
- ein Umsetzungsdatum, wenn die Maßnahme zwar als sinnvoll angesehen wird, aber erst zum angegebenen Datum umgesetzt wird.

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Maßnahme	Erfüllt?
Ausweistragepflicht für Besucher	Ja
Ausweistragepflicht für Mitarbeiter	Ja
Personenkontrolle am Eingang	Ja
Protokollierung der Besucher (Besucherbuch)	Ja

Maßnahme	Erfüllt?
Protokollierung der Schlüsselausgabe (Schlüsselbuch)	Ja
Sorgfältige Auswahl des Reinigungspersonals	Ja
Einrichtung von Schutz- und Sicherheitszonen	Ja
Festlegung der zugangsberechtigten Personen	Ja
Absicherung von Gebäudeschächten	n/a
Alarmanlage	Ja
Automatisches Zugangskontrollsystem	Nein
Bewegungsmelder	Ja
Manuelles Schließsystem	Ja
Schließsystem mit Zugangscode	Nein
Sicherheitsschlösser	Ja
Videoüberwachung der Zugänge	Ja
Protokollierung der Zu- und Abgänge	Nein

1.2 Zugangskontrolle

Maßnahme	Erfüllt?
Revisionsfähigkeit der Zugangsberechtigungen	Ja
Passwortrichtlinie (Regelung von Passwortregeln und Wechsel)	Ja
Multi-Faktor-Authentifizierung	Ja
Zertifizierte Dienstleister für Akten- und Datenvernichtung	Ja
Regelungen zur Verlustmeldung und Reaktionen auf Datenträgerverlust	Ja
Netzwerksegmentierung	Nein
NAC - Network Access Control	Ja
Automatische Bildschirmsperre	Ja
Cloud-Zugangskontrolle über IAM	Ja

1.3 Zugriffskontrolle

Maßnahme	Erfüllt?
Minimierte Anzahl von Administratoren	Ja
Sichere Aufbewahrung von Datenträgern	Ja
Sichere Verwaltung von Benutzerrechten	Ja
Regelmäßige Überprüfung der Berechtigungen	Ja
Revisionsfähiges Rollen-, Berechtigungs- und Nutzerkonzept	Ja
Datenträger-Vernichtung nach DIN 66399	Ja
Externer Aktenvernichter (DIN 32757)	Ja
Physische Löschung von Datenträgern vor Wiederverwendung	Nein
Protokollierung der Datenvernichtung	Ja
Protokollierung der Eingabe, Veränderung und Löschung von Daten	Ja
Verschlüsselung von Datenträgern	Ja
Verschlüsselung von mobilen Geräten	Ja
Beschränkung der freien Abfragemöglichkeiten von Datenbanken	Ja
Zeitliche Begrenzung der Zugriffsmöglichkeiten	Ja

1.4 Trennbarkeit von Daten

Maßnahme	Erfüllt?
Trennung von Datenbanken durch Berechtigungen	Ja
Berechtigungskonzept für Anwendungen, Laufwerke und Dateien	Ja
Organisatorische Berücksichtigung der Mandantentrennung	Ja
Datensätze sind mit Zweckattributen versehen	Ja
Trennung von Produktiv- und Testsystem	Ja
Mandantenfähigkeit relevanter Anwendungen, inkl. Cloud-Ressourcen	Ja
Physikalisch getrennte Systeme	Nein
Logische Trennung der Cloud-Instanzen	Ja
Trennung durch getrennte Verschlüsselung	Ja

Maßnahme	Erfüllt?
Verwendung von Software, die eine buchhalterische Mandantentrennung ermöglicht	Ja

1.5 Pseudonymisierung

Maßnahme	Erfüllt?
Interne Anweisung, personenbezogene Daten im Falle der Weitergabe oder nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren	Ja
Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System	Nein

---

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Maßnahme	Erfüllt?
Festlegung der Übermittlungswege und der Datenempfänger	Ja
Organisatorische Regelungen zur Einrichtung und Befristung von Fernzugriffen (z. B. VPN)	Ja
Regelungen zum datenschutzgerechten Einsatz mobiler Datenträger	Ja
Regelungen zum datenschutzgerechten E-Mail-Versand	Ja
Nutzung von Cloud-Anbietern (z. B. Office365, Google Cloud)	Ja
Nutzung der OVH Cloud als primäre Hosting-Infrastruktur	Ja
Nutzung einer eigenen Serverinfrastruktur	Nein
Nutzung von hosted Servern eines Dienstleisters	Ja
Dokumentation der Abruf- und Übermittlungsvorgänge	Ja
Dokumentation der Datenempfänger, Überlassungs- und Löschfristen	Ja
Automatisierte Überwachung nach außen offener Ports, Protokolle und Dienste	Ja
Protokollierung der Datenübermittlung inkl. Abrufe und Empfänger	Ja
Einrichtung von VPN-Tunneln	Ja
E-Mail-Verschlüsselung	Nein
Sicheres Löschen	Ja

Maßnahme	Erfüllt?
Überprüfung von Datenträgern auf Virenbefall	Ja
Zeitbegrenzung von Zugriffsmöglichkeiten	Ja
Protokollierung der autorisierten Weitergabe und Entfernung von Datenträgern	Ja
Protokollierung der Kopie von Datenträgern	Ja
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	Ja

2.2 Datenintegrität

Maßnahme	Erfüllt?
Sicherung der Software durch digitale Signaturen oder Hashwerte	Ja
Verschlüsselung der Datenträger	Ja
Verschlüsselung der internen Übertragungswege	Ja
Verschlüsselung von Dateien und Datenbanken	Ja
Kontrolle und Trennung von System- und User-Aktivitäten	Ja

---

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Maßnahme	Erfüllt?
Notfallplan für die eingesetzten Systeme	Ja
Backup- und Recovery-Konzept	Ja
Kontrolle des Sicherungsvorgangs	Ja
Test der Datenwiederherstellung	Ja
Automatisierte Systemüberwachung und Alarmierung	Ja
Feuer- und Rauchmeldeanlagen	Ja
USV - Unterbrechungsfreie Stromversorgung	Ja
Trennung von Produktiv- und Testsystem	Ja
Nutzung der OVH Cloud-Infrastruktur mit SLA für Hochverfügbarkeit	Ja

Maßnahme	Erfüllt?
Geografisch verteilte Rechenzentren des Cloud-Anbieters	Ja
Cloud-basiertes Backup- und Recovery-Konzept	Ja
Datenverarbeitung ausschließlich in EU-Rechenzentren	Ja

---

4 Wiederherstellbarkeit und Zuverlässigkeit (Art. 32 Abs. 1 lit. c DS-GVO)

4.1 Wiederherstellbarkeit

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Maßnahme	Erfüllt?
Notfallplan	Ja
Mehrstufiges Backup- und Restorekonzept	Ja
Sicherheits-Vorfall-Management	Ja
Notfallkonzept	Ja
Backup- und Restoreautomatisierung	Ja
Nutzung der Cloud-Anbieter-Disaster-Recovery-Funktionen	Ja
Regelmäßige Tests der Wiederherstellungsprozesse in der Cloud-Umgebung	Ja

4.2 Zuverlässigkeit

Gewährleistet das zuverlässige Funktionieren der Datenverarbeitungssysteme

Maßnahme	Erfüllt?
Mindestens jährliche und dokumentierte Überprüfung der TOM	Ja
Regelung zur Reaktion auf Störungen	Ja
SLA für IT-Leistungen	Ja
Zentrale Beschaffung von Hard- und Software	Nein
Virenschutz	Ja
Malwarescan	Ja

Maßnahme	Erfüllt?
Penetrationstests	Nein
Regelmäßiges und zeitnahes Patch-Management	Ja
MDM (Mobile Device Management) - Umfassendes System zur zentralen Verwaltung, Sicherung und Überwachung von mobilen Endgeräten inklusive Durchsetzung von Sicherheitsrichtlinien, Fernlöschung, Verschlüsselungsmanagement und Anwendungskontrolle	Ja

---

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

5.1 Auftragskontrolle

Gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahme	Erfüllt?
Auftragsverarbeitungsvertrag (AVV)	Ja
Laufende Überprüfung des Auftragnehmers	Ja
Prüfung der TOM des Auftragnehmers vor erstmaliger Datenübertragung	Ja
Sichere Datenvernichtung nach Auftragsende	Ja
Vereinbarung von Kontrollrechten	Ja
Vereinbarung von Kontrollrechten für lector.ai	Ja
Vereinbarung von Vertragsstrafen	Nein
Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit nach DSGVO	Ja
Sorgfältige Auswahl des Auftragnehmers	Ja
Sorgfältige Vertragsgestaltung	Ja
Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber	Ja
Schriftliche Weisungen an den Auftragnehmer	Ja
Regelungen zum Einsatz weiterer Subunternehmer	Ja
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	Ja

Maßnahme	Erfüllt?
Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus bei längerer Zusammenarbeit	Ja
Protokollierung und Kontrolle der ordnungsgemäßen Vertragsausführung	Ja

5.2 Datenschutz-Management

Gewährleistet die Einhaltung der DSGVO durch die Etablierung entsprechender Prozesse

Maßnahme	Erfüllt?
Interner/externer Datenschutzbeauftragter (Kontaktdaten in AVV)	Ja
Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet	Ja
Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)	Ja
Interner Informationssicherheitsbeauftragter	Ja
Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	Ja
Die Organisation kommt den Informationspflichten nach Art. 13, 14 DSGVO nach	Ja
Formaler Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener	Ja
Software-Lösungen für Datenschutz-Management im Einsatz	Nein
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz	Ja
Sicherheitszertifizierung nach ISO 27001, BSI IT Grundschutz oder ISIS12	Nein
Alternatives Informationssicherheitskonzept	Ja
Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (mindestens jährlich)	Ja
Berücksichtigung der ISO 27001, 27017, 27018 Zertifizierungen des Cloud-Anbieters	Ja
Abschluss eines AVV mit dem Cloud-Anbieter OVH	Ja
Jährliche Überprüfung der Compliance des Cloud-Anbieters	Ja

5.3 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Maßnahme	Erfüllt?
Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Datenpannen	Ja

Maßnahme	Erfüllt?
Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	Ja
Einbindung von DSB in Sicherheitsvorfälle und Datenpannen	Ja
Einbindung von ISB in Sicherheitsvorfälle und Datenpannen	Ja
Dokumentation von Sicherheitsvorfällen und Datenpannen, z.B. via Ticketsystem	Ja
Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	Ja
Einsatz von Firewall und regelmäßige Aktualisierung	Ja
Einsatz von Spamfilter und regelmäßige Aktualisierung	Ja
Einsatz von Virenscanner und regelmäßige Aktualisierung	Ja
Intrusion Detection System (IDS)	Ja
Intrusion Prevention System (IPS)	Ja

5.4 Datenschutzfreundliche Voreinstellungen

Gemäß Art. 25 Abs. 2 DSGVO

Maßnahme	Erfüllt?
Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	Nein
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	Ja

---

Die Richtigkeit der Angaben wird bestätigt:

Benjamin von Ardenne

Geschäftsführer der lector.ai GmbH

Bremen, 18.11.2025

Anlage 3: Genehmigte Subunternehmer

> **Info**: Diese Anlage ist Bestandteil der Auftragsverarbeitungsvereinbarung (AVV) und listet alle genehmigten Subunternehmer auf. Die Serverstandorte sind bewusst auf EU/DE-Regionen beschränkt, um DSGVO-Konformität zu gewährleisten. Der Stand des Dokuments und die Subunternehmer-Liste werden regelmäßig auf Aktualität überprüft.

Stand: 29. Juli 2025

Zum Zeitpunkt der Beauftragung genehmigt der Auftraggeber den Einsatz folgender Subunternehmer für die nachfolgend dargestellten Tätigkeiten:

Name/ Firma	**Anschrift**	**Serverstandort(e)**	**Tätigkeit**
Google Cloud EMEA Limited**1	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland	Frankfurt (europe-west3), Belgien (europe-west1)	Hosting von virtuellen Maschinen für Entwicklung, Monitoring und Betriebs-Support, Optional Betrieb von LLM-Modellen (u.a. Anthropic, Gemini und Llama Modelle) über Vertex Ai.
OVH GmbH**2	Oskar-Jäger-Str. 173/ K6, 50825 Köln, Deutschland	Frankfurt (DE), Graveline (FR)	Betrieb der lector.ai Platform-as-a-Service und der LLM-Proxy-Services.
Azure OpenAI Service**3	Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin 18, D18 P521, Ireland	Deutschland (Germany West Central)	Betrieb von DSGVO-konformen GPT-4 und ähnlichen Large Language Models über den Azure OpenAI Service.
n8n GmbH**4	Novalisstr. 10, 10115, Berlin, Germany	Frankfurt (DE)	Optional: Betrieb der n8n-Workflow-Automatisierungsplattform für die Integration von

Name/ Firma	Anschrift	Serverstandort(e)	Tätigkeit
			Geschäftsprozessen und Datenflüssen.
HubSpot Ireland Limited**5	One Dockland Central, Guild Street, Dublin 1, Ireland	Frankfurt (EU Central)	CRM-System, Kundenkommunikation, Marketing E-Mails und Verwaltung von Kundenbeziehungen.
Stripe Payments Europe Ltd.**6	The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland	Europa (EU-Region, Dublin)	Abrechnung und Zahlungsabwicklung für die Dienste von lector.ai.

1. Die Auftragsverarbeitung durch den Subunternehmer Google LLC wird durch das Data Processing Agreement https://cloud.google.com/terms/data-processing-terms geregelt und fällt unter die Standard-Datenschutz-Klauseln (SDK) https://cloud.google.com/terms/sccs/eu-c2p. Zusätzlich ist Google Cloud seit Oktober 2023 nach dem EU-US Data Privacy Framework zertifiziert, was einen weiteren Rechtsrahmen für den Datentransfer zwischen der EU und den USA bietet.

   Für die Nutzung der Google Cloud Vertex AI gelten die Zusatzbedingungen der Gemini API (https://ai.google.dev/gemini-api/terms?hl=de). Für diese kostenpflichtigen Dienste gilt insbesondere: „Wenn Sie kostenpflichtige Dienste nutzen, verwendet Google Ihre Prompts (einschließlich zugehöriger Systemanweisungen, im Cache gespeicherter Inhalte und Dateien wie Bilder, Videos oder Dokumente) oder Antworten nicht, um die Produkte von Google zu verbessern, und verarbeitet Ihre Prompts und Antworten in Übereinstimmung mit dem Zusatz zur Datenverarbeitung für Produkte, bei denen Google ein Datenauftragsverarbeiter ist (Google Data Processing Addendum for Products Where Google is a Data Processor). Diese Daten können in jedem Land, in dem Google oder seine Vertreter Einrichtungen unterhalten, vorübergehend oder im Cache gespeichert werden."

   Google Cloud verschlüsselt die Daten standardmäßig serverseitig, bevor sie auf ein Laufwerk geschrieben werden. Bei der Übertragung von und zum Server findet TLS-Verschlüsselung statt, inaktive Daten werden seitens des Cloud Anbieters via AES256 verschlüsselt. Das Verschlüsselungsschlüsselmanagement wird von lector.ai verwaltet (Cloud Key Management Service).

   Google ist nach ISO27018 zertifiziert und wird jährlich auditiert. Weitere Informationen finden Sie unter: https://cloud.google.com/security/compliance/iso-27018?hl=de Zertifikate können über den Compliance Reports Manager heruntergeladen werden: https://cloud.google.com/security/compliance/compliance-reports-manager#/ReportType=Certificate&ProductArea=Google_Cloud

   Lector.ai bietet über Google Vertex Ai verschiedene LLM Modelle an, die ausschließlich auf Servern innerhalb der Europäischen Union betrieben werden. Auf der Plattform ist eindeutig

gekennzeichnet, wo die jeweils ausgewählten Modelle betrieben werden. Es liegt in der Wahl des Kunden, welche Modelle und EU-Standorte gewählt werden.

2. Die Auftragsverarbeitung durch den Subunternehmer OVH GmbH wird durch das Data Processing Agreement https://us.ovhcloud.com/legal/data-processing-agreement/ geregelt.

   Lector.ai bleibt alleiniger Eigentümer der von ihm im Rahmen der OVH Dienstleistungen gespeicherten Daten. OVH greift weder auf diese Daten zu noch werden sie verwendet, solange dies nicht für die korrekte Ausführung der Dienstleistungen notwendig ist, und auch dann nur innerhalb der technischen Grenzen dieser Dienstleistungen. OVH ist es untersagt, die genannten Daten weiterzuverkaufen oder für eigene Zwecke (zum Beispiel Datamining, Profiling oder Direktmarketing) zu verwenden.

   OVH ist nach ISO 27001, ISO 27017 und ISO 27018 zertifiziert. Weitere Informationen finden Sie unter: https://www.ovhcloud.com/de/compliance/iso-27001-27017-27018/

3. Im Fall von OpenAI API-Diensten (wie dem Microsoft Azure OpenAI Service), werden keine Daten für das Training von Modellen oder für andere Zwecke von OpenAI verwendet, es sei denn, es wurde ausdrücklich eine Erlaubnis dazu erteilt. Bei der Nutzung über Azure wird die Datenverarbeitung durch Microsofts Datenschutzrichtlinien (s. Microsoft DPA in Anhang 2) geregelt. Microsoft speichert und verarbeitet die Daten nicht für eigene Zwecke und sichert zu, dass die Kundendaten vertraulich behandelt werden.

   Quelle: https://learn.microsoft.com/de-de/legal/cognitive-services/openai/data-privacy (Stand: 23. September 2024)

   Wichtige Datenschutzaspekte des Azure OpenAI Service:

   - Alle Daten werden ausschließlich in der EU-Region (Germany West Central) verarbeitet
   - Microsoft implementiert strenge Zugriffskontrollen und Protokollierung für Systemadministratoren
   - Automatische Verschlüsselung der Daten im Ruhezustand (Storage) und während der Übertragung (TLS 1.2)
   - Keine Speicherung von Prompts oder Antworten nach Abschluss der Verarbeitung
   - Konformität mit ISO 27001, SOC 1/2/3, und DSGVO-Anforderungen
   - Microsoft bietet standardmäßig Customer Managed Keys (CMK) für zusätzliche Kontrolle
   - Regelmäßige Sicherheitsaudits und Penetrationstests durch unabhängige Dritte
   - Transparente Incident Response und Breach Notification Prozesse gemäß DSGVO

4. Die Auftragsverarbeitung durch den optionalen Subunternehmer n8n GmbH wird durch das Data Processing Agreement https://n8n.io/legal/#data geregelt. Die n8n GmbH ist ein in Deutschland ansässiges Unternehmen, das eine Workflow-Automatisierungsplattform bereitstellt. Sämtliche Datenverarbeitung findet in der EU statt, speziell im Rechenzentrum in Frankfurt.

   Die n8n-Plattform kann optional zur Automatisierung von Geschäftsprozessen und zur Integration verschiedener Systeme eingesetzt werden. Die Daten werden während der Übertragung mittels TLS 1.2/1.3 und im Ruhezustand mittels AES-256 verschlüsselt. n8n ist nach ISO 27001 zertifiziert und wird regelmäßig auf Sicherheitsstandards überprüft.

Die Nutzung der n8n-Plattform ist optional und erfolgt nur nach expliziter Beauftragung durch den Kunden.

5. Die Auftragsverarbeitung durch den Subunternehmer HubSpot Ireland Limited wird durch das Data Processing Agreement https://legal.hubspot.com/dpa geregelt. HubSpot ist nach ISO 27001, SOC 2 Typ II und verschiedenen anderen Sicherheitsstandards zertifiziert.

   HubSpot wird für die Verwaltung von Kundenbeziehungen (CRM), für Marketing-E-Mails und für die Kommunikation mit Kunden eingesetzt. Die Datenverarbeitung findet ausschließlich in der EU statt (Rechenzentrum in Frankfurt).

   Die Daten werden während der Übertragung mit TLS 1.2 und im Ruhezustand mit AES-256 verschlüsselt. HubSpot bietet umfangreiche Kontrollen zum Schutz personenbezogener Daten gemäß DSGVO und stellt entsprechende Funktionen zur Erfüllung von Betroffenenrechten bereit.

   Die HubSpot-Plattform respektiert die EU-Standardvertragsklauseln (SCCs) und ermöglicht die Löschung oder Anonymisierung von Kundendaten gemäß den geltenden Datenschutzbestimmungen.

6. Die Auftragsverarbeitung durch den Subunternehmer Stripe Payments Europe Ltd. wird durch das Data Processing Agreement https://stripe.com/de/legal/dpa geregelt. Stripe ist nach PCI DSS Level 1, ISO 27001, SOC 1 Typ II und SOC 2 Typ II zertifiziert.

   Stripe wird für die Abrechnung und Zahlungsabwicklung der lector.ai-Dienste eingesetzt. Die Datenverarbeitung erfolgt in der EU-Region (Dublin). Stripe implementiert branchenführende Sicherheitsmaßnahmen zum Schutz von Zahlungsdaten und personenbezogenen Daten.

   Die Daten werden während der Übertragung mit TLS 1.2+ und im Ruhezustand mit AES-256 verschlüsselt. Stripe erfüllt alle Anforderungen der DSGVO und stellt Tools zur Verfügung, um Betroffenenrechte zu gewährleisten.

   Stripe behandelt alle Daten vertraulich und verwendet sie ausschließlich zur Bereitstellung der Zahlungsdienste, ohne sie für eigene Zwecke zu nutzen oder weiterzuverkaufen.