

Analyse: KI- Anwendung von Mistral Stand: September 2025

Anmerkung: Da es sich um eine sehr umfangreiche Analyse handelt, sind einige Passagen nur in Stichworten angegeben.

I. Zu bewertendes Verfahren / Tool und Zweckbestimmung

Das erst im Jahr 2023 gegründete KI Unternehmen Mistral AI mit Firmensitz in 75001 Paris, Frankreich, will mit seinem in Frankreich entwickelten Produkten und Dienstleistungen im Bereich KI den US-amerikanischen Unternehmen Konkurrenz machen.

Mistral AI bietet eine Reihe von Produkten und Dienstleistungen, zu den Hauptprodukten gehören:

1. **Mistral Large Language Models:** Diese Modelle sind darauf ausgelegt, natürliche Sprache zu verstehen und zu generieren. Sie können für eine Vielzahl von Anwendungen eingesetzt werden, darunter Textgenerierung, Übersetzungen, Zusammenfassungen und mehr.
2. **Mistral Cloud Services:** Diese Dienstleistungen bieten skalierbare und sichere Lösungen für Unternehmen, die die Mistral-Modelle in der Cloud nutzen möchten. Sie umfassen Hosting, Wartung und Skalierung der Modelle.
3. **Mistral Code Models:** Diese Modelle sind speziell darauf ausgelegt, Code zu verstehen und zu generieren. Sie können bei der Automatisierung von Code-Review-Prozessen, der Erstellung von Code-Snippets und der Fehlerbehebung helfen.
4. **Mistral API:** Diese API ermöglicht es Entwicklern, die Mistral-Modelle in ihre eigenen Anwendungen zu integrieren. Sie bietet eine einfache und flexible Möglichkeit, die Leistungsfähigkeit der Mistral-Modelle zu nutzen.
5. **Mistral Custom Solutions:** Für spezifische Anforderungen bieten sie maßgeschneiderte Lösungen an, die auf die Bedürfnisse des Kunden zugeschnitten sind. Dies kann die Entwicklung von benutzerdefinierten Modellen, die Integration in bestehende Systeme und die Bereitstellung von Schulungen und Support umfassen.

Le Chat (ein mit Chat GPT vergleichbarer Chatbot) fällt unter die Kategorie der Mistral Large Language Models. Le Chat kann für eine Vielzahl von Anwendungen eingesetzt werden, darunter Textgenerierung, Übersetzungen, Zusammenfassungen und mehr.

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 2

Die Plattform (**La Plateforme**), auf der Le Chat läuft, fällt unter die Kategorie Mistral Cloud Services. Diese Dienstleistungen umfassen Hosting, Wartung und Skalierung der Modelle, die es Unternehmen ermöglicht, die KI-Modelle nahtlos in ihre Anwendungen zu integrieren.

Diese Datenschutzfolgeabschätzung umfasst nicht sämtliche Produkte von Mistral sondern nur die ersten beiden Dienstleistungen des LLM und des Cloud Services. Sollten weitere der oben aufgeführten Dienstleistungen von Mistral benötigt werden, muss zunächst eine erneute Datenschutzfolgeabschätzung erfolgen.

1. Betroffenengruppen deren personenbezogene Daten verarbeitet werden

Die bei Vertragsschluss erhobenen Daten – Name des Geschäftsführers und der IT-Leitung

Bei Nutzung – Mailadresse und IP des Nutzers

Alle Personen – da das LLM keine Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten treffen kann. Bei Eingabe personenbezogener Daten werden die auch verarbeitet.

2. Art der Daten

In der Datenschutzerklärung von Mistral findet sich unter **2.1.** folgende Auflistung:

(Auszug)

Daten, die Sie uns direkt zur Verfügung stellen

Kategorie der persönlichen Daten	Wann sammeln wir Ihre persönlichen Daten ?
Identitätsdaten , wie Ihr Vor- und Nachname. Kontodaten , wie die Mittel, um Ihr Passwort abzurufen und Ihr Konto zu überprüfen. Kontaktdaten , wie z.B. Ihre E-Mail-Adresse. Contract Data , wie das Mistral AI Product das sie abonnieren.	Wenn Sie Ihr Mistral AI-Konto erstellen und ein Mistral AI Produkt abonnieren.
Kontaktdaten , wie z.B. Ihre E-Mail-Adresse.	Wenn Sie abonnieren, um unsere Mitteilungen zu erhalten.

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 3

Kategorie der persönlichen Daten	Wann sammeln wir Ihre persönlichen Daten ?
Zahlungs- und Rechnungsinformationen , wie Ihre Rechnungen oder Ihre Rechnungsadresse.	Wenn Sie ein bezahltes Mistral AI Produkt abonnieren
"Eingeben " , alle Daten, die Sie zur Generierung einer Ausgabe bereitstellen, wie z. B. Aufforderungen oder Feinabstimmungsdaten. „Feedback“ , alle Informationen, die Sie angeben, wenn Sie eine Ausgabe bewerten, wie "Daumen hoch" oder "Daumen nach unten" und die zugehörige Eingabe und Ausgabe.	Wenn Sie die Mistral AI Produkte verwenden

2.2. Persönliche Daten, die bei der Nutzung der Mistral AI Produkte generiert werden

Kategorie der persönlichen Daten	Wann sammeln wir Ihre persönlichen Daten ?
"Technische Daten " , alle Protokolle oder technischen Daten, die Ihr Browser und Gerät automatisch senden, wenn Sie die Mistral AI Produkte verwenden, z. B. Ihre IP-Adresse oder die Art des von Ihnen verwendeten Netzwerkprotokolls. Hier aufgeführten Cookies (Liste befindet sich im Anschluss an 2.3 des Auszugs aus der Datenschutzerklärung – Anmerkung Verfasserin) „Nutzungsdaten " , alle Daten, die sich auf die Verwendung der Mistral AI Produkte beziehen. „Ausgang“ , Inhalte, die von den Mistral AI-Produkten basierend auf Ihrer Eingabe generiert werden.	Wenn Sie die Mistral AI Produkte verwenden

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 4

2.3. Persönliche Daten, die uns (gemeint ist Mistral – Anmerkung der Verfasserin) indirekt zur Verfügung gestellt werden

Daten öffentlich im Internet. Unsere Modelle für künstliche Intelligenz sind auf Daten geschult, die im Internet öffentlich verfügbar sind und personenbezogene Daten enthalten können, auch wenn wir gute Praktiken verwenden, um solche persönlichen Daten herauszufiltern.

Daten von Dritten:

- **Hugging face Plattform.** Wenn Sie unsere Modelle für künstliche Intelligenz auf Hugging Face herunterladen, sammeln wir Ihren Benutzernamen und Ihre E-Mail-Adresse, um unsere Lizenz durchzusetzen und Ihnen Mitteilungen über unsere neuen Modelle zu senden.
- **Inhalte Dritter.** Wenn Sie bestimmte Funktionen verwenden, die mit Mistral AI-Produkten von Drittanbietern interagieren, wie Websuche oder verifizierte Neuigkeiten auf Le Chat, können wir Inhalte von Dritten auf Le Chat anzeigen, z. B. Links, Thumbnails oder Snippets (die "**In Inhalt der Dritten**"). Dieser Inhalt wird angezeigt, um das Ergebnis besser zu verstehen. Wenn Sie personenbezogene Daten in Ihren Input aufnehmen, können auch personenbezogene Daten im Inhalt der Dritten Partei erscheinen. Wir verwenden diese Inhalte von Dritten nicht, um unsere Modelle zu trainieren.

(Ende des Auszugs)

Laut der Cookierichtlinie von Mistral vom 27.05.2025 werden folgende Cookies genutzt:

Technisch erforderliche Cookies.

- Cloudflare zum Zweck der Sicherheits- und Ratenbegrenzungsregeln.
- Intercom zum Zweck der Unterstützung des Chatbots
- Mistral AI zum Zweck der Spracheinstellungen
- Ory zum Zweck der Authentifizierung

Analytik:

- Google Analytics zum Zweck der Zählung der Besucher und Messung der Websiteleistung
- Posthog zum Zweck der Analyse und Verbesserung der Interaktion mit der Website

Marketing:

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 5

- X zum Zweck der Verfolgung Ihrer Interaktionen mit den Beiträgen oder Anzeigen, die wir auf X anzeigen, um die Leistung unserer Marketingkampagnen zu messen.
- Meta zum Zweck der Verfolgung Ihrer Interaktionen mit den Beiträgen oder Anzeigen, die wir auf Meta anzeigen, um die Leistung unserer Marketingkampagnen zu messen.

(Auszug Datenschutzerklärung Mistral)

3. Warum nutzen wir Ihre persönlichen Daten?

Warum wir Ihre persönlichen Daten verwenden	Kategorien personenbezogener Daten	Rechtsgrundlage
Um die Mistral-KI-Produkte bereitzustellen und zu erhalten, die Ihnen unter den Bedingungen in unseren Nutzungsbedingungen und den geltenden Zusatzbedingungen zur Verfügung gestellt werden	Ihre zivilen Identitätsdaten Ihre Kontodaten Ihre Vertragsdaten Ihre technischen Daten Ihr Input, Output und Feedback Ihre Nutzungsdaten. <i>Bitte beachten Sie, dass wir einen Teil Ihrer IP-Adresse verwenden, um Ihre Erfahrung zu verbessern, z. B. um Ihnen genauere Ergebnisse zu bieten, je nachdem, wo Sie unsere Mistral-KI-Produkte verwenden. Sie können diese Verarbeitung jederzeit über Ihre Benutzerpräferenzen auf Ihrem Mistral AI Account deaktivieren.</i>	Die Vertragserfüllung zwischen Ihnen und Mistral AI
Debugging	Ihr Input, Output und Feedback	Die Vertragserfüllung zwischen Ihnen und Mistral AI.

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 6

Warum wir Ihre persönlichen Daten verwenden	Kategorien personenbezogener Daten	Rechtsgrundlage
So erstellen und verwalten Sie Ihr Mistral AI Account	Ihre zivilen Identitätsdaten Ihre Kontodaten Ihre Vertragsdaten	Die Vertragserfüllung zwischen Ihnen und Mistral AI.
Um Kundensupport zu bieten, einschließlich Debugging und Fixierung von Fehlern, die von Ihnen gemeldet wurden	Ihre zivilen Identitätsdaten Ihre Kontaktdaten Ihr Feedback Ihr Input und Output	Die Vertragserfüllung zwischen Ihnen und Mistral AI.
Um die Sicherheit und Integrität der Mistral AI Produkte zu steuern	Ihre zivilen Identitätsdaten Ihre Kontodaten Ihre technischen Daten Ihre Kontaktdaten Ihre Nutzungsdaten	Um unseren gesetzlichen Verpflichtungen nachzukommen. Unsere legitimen Interessen bei der Verwaltung der Sicherheit und Integrität der Mistral AI-Produkte.
Um mit Ihnen zu kommunizieren, einschließlich, um Ihnen Newsletter oder Nicht-Marketing-Kommunikation über die Mistral AI Products zu senden	Ihre zivilen Identitätsdaten Ihre Kontaktdaten	Ihre Zustimmung, für Marketingkommunikation. Die Erfüllung der Vereinbarung für alle Nicht-Marketing-Kommunikation (z.B. um Ihnen Benachrichtigungen über Änderungen zu unseren Bedingungen zu senden).
Um die Mistral AI-Produkte zu verbessern oder neue Produkte zu entwickeln (aber Modelltraining auszuschließen), wie zum Beispiel, um Forschung zu betreiben oder aggregierte und anonyme Statistiken zu erstellen	Ihre zivilen Identitätsdaten Ihr Feedback Ihr Input und Output Aggregierte und	Unser berechtigtes Interesse daran, die Mistral-KI-Produkte kontinuierlich zu verbessern und neue Features einzuführen.

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 7

Warum wir Ihre persönlichen Daten verwenden	Kategorien personenbezogener Daten	Rechtsgrundlage
Um unsere Modelle für künstliche Intelligenz (große Sprachmodelle) zu trainieren, um Fragen zu beantworten, Text zu generieren, Text zu übersetzen, zusammenzufassen und zu korrigieren, Text zu klassifizieren, Gefühle zu analysieren usw. nach Kontext, Eingaben (E-Mails, Briefe, Berichte, Computercode usw.) und Outputs.	Persönliche Daten, die in den im Internet öffentlich verfügbaren Daten enthalten sind, trotz unserer Bemühungen, solche persönlichen Daten herauszufiltern Ihr Eingang und Ausgang, vorbehaltlich Ihrer Opt-out. <i>Bitte beachten Sie, dass wir Ihre Input und Output nicht verwenden, um unsere Modelle für künstliche Intelligenz zu schulen, wenn Sie Le Chat Team, Le Chat Enterprise oder die kostenpflichtige Version unserer APIs verwenden. Wenn Sie einen Drittanbieter-Dienst mit den Mistral AI-Produkten verbinden, verwenden wir diesen Drittanbieterdienst nicht, um unsere Modelle der künstlichen Intelligenz zu schulen.</i> Ihr Feedback.	Unser berechtigtes Interesse an der Entwicklung und Bereitstellung modernster Großsprachmodelle als Teil der Mistral AI Products.
Um unsere Nutzungsbedingungen und Lizenzen zu verwalten und durchzusetzen, einschließlich der Mäßigung und Missbrauchsüberwachung	Ihre zivilen Identitätsdaten Ihre Kontodaten Ihre Kontaktdaten Ihr Input und Output Ihr Feedback	Die Vertragserfüllung zwischen Ihnen und Mistral AI.

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 8

Warum wir Ihre persönlichen Daten verwenden	Kategorien personenbezogener Daten	Rechtsgrundlage
Um unsere Handelsbeziehungen mit Ihnen zu verwalten, einschließlich der Abwicklung von Zahlungen und der Verwaltung der Rechnungsstellung	Ihre zivilen Identitätsdaten Ihre Kontodaten Ihre Kontaktdaten Ihre Zahlungs- und Rechnungsinformationen	Die Leistung des Abkommens zwischen Ihnen und Mistral AI. Unsere gesetzlichen Pflichten.
Die Auseinandersetzungen zwischen Ihnen und Mistral AI untersuchen und lösen	Geschieht und je nach Streit: Ihre Identität Ihre Kontodaten Ihre Kontaktdaten Ihre Vertragsdaten Ihre technischen Daten Ihre Nutzungsdaten Ihr Input, Output und Feedback Alle anderen Daten, die für die Untersuchung oder Beilegung des Streits erforderlich sind.	Unser berechtigtes Interesse am Schutz und Ausübung unserer Rechte. Die Erfüllung des Abkommens zwischen Ihnen und Mistral AI.
Um auf Ihre Wünsche zu antworten, Ihre Rechte an Ihren persönlichen Daten auszuüben	Ihre zivilen Identitätsdaten Ihre Kontodaten Ihre Kontaktdaten Alle anderen persönlichen Daten, die in Ihrer Datenerhebung enthalten sind	Unsere gesetzliche Verpflichtung, auf Ihre Wünsche zu antworten.

3. An der Verarbeitung beteiligten Komponenten (Systeme und Dienste sowie Prozesse)

- **Microsoft Azure**, Cloud-Infrastruktur, Schweden, Norwegen

Produkte: Le Chat, La Plateforme, Mistral Code

- **Google Cloud Platform**, Cloud-Infrastruktur, Irland, Vereinigte Staaten

Produkte: Le Chat, La Plateforme (US-API)

- **Stripe**, Zahlung und Abrechnung, Vereinigte Staaten

Produkte: Alle Produkte im Rahmen eines kostenpflichtigen Abonnements

- **Lago**, Abrechnung, EWR

Produkte: Alle Produkte im Rahmen eines kostenpflichtigen Abonnements

- **Blackforest Labs**, Bildgenerierung, Vereinigte Staaten

Produkte: Le Chat, Agents API

- **Brave**, Websuche, Vereinigte Staaten

Produkte: Le Chat, Agents API

- **Cerebras**, Flash Answers, Vereinigte Staaten

Produkte: Le Chat

- **Foundrylabs, Inc.**, Code-Interpreter (E2B.dev), Frankreich, Belgien, Niederlande

Produkt: Le Chat, Agents API

- **Intercom**, Benutzersupport, EWR

Produkte: Alle Produkte

- **Kong**, Sicherheit (API), EWR

Produkte: La Plateforme

- **Ory**, Benutzerauthentifizierung, EWR

Produkte: Alle Produkte

- **Merge.dev**, Konnektoren auf Le Chat – Übertragung von ACL und Daten vom Drittanbieter-Dienst zu Le Chat, Vereinigte Staaten

Produkte: Le Chat. Merge verarbeitet die Daten nur, wenn der Nutzer die Konnektorfunktion auf Le Chat aktiviert

- **Resend**, E-Mail-Kommunikation, Irland

Produkte: Alle Produkte

- **Twilio**, Telefonnummernüberprüfung, Vereinigte Staaten

Produkte: Alle Produkte

II. Schutzbedarfsbestimmung

Gewährleistungsziele:

Technische und organisatorische Maßnahmen sollen eine rechtskonforme Verarbeitung gewährleisten. Bei der vorliegenden Prüfung sind insbesondere die Gewährleistungsziele der Vertraulichkeit, der Nichtverkettung und der Transparenz betroffen.

Vertraulichkeit bedeutet, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann. Dieses Gewährleistungsziel ist dann äußerst betroffen, wenn Input und Output zum Training der KI verwandt werden.

Das Ziel ist ebenfalls betroffen, wenn Le Chat über die Mistralplattform La Plattform genutzt wird, weil die Plattform auf Servern gehostet ist die us- amerikanischen Tech-Firmen wie Microsoft und Google gehören. Gemäß us-amerikanischer Gesetze wie z.B. dem Cloud Act und dem Patriot Act müssen diese Firmen den US-Behörden auch dann Zugriff auf die Server gewähren, wenn diese sich physisch in Europa befinden.

Das Gleiche gilt für das Gewährleistungsziel der Nichtverkettung, d.h. der Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Auch dieses Ziel ist bei Nutzung der Daten zu Trainingszwecken betroffen, denn eben das Verketteten von Informationen ist ein Kernstück der Arbeit der generativen KI.

Das Gewährleistungsziel der Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

Die sich zum heutigen Zeitpunkt – September 2025 - auf dem Markt befindlichen vergleichbaren us-amerikanischen Produkte zeichnen sich durchgehend durch ihre Intransparenz bei der Verarbeitung von Daten aus.

Schutzbedarf/ Schadenshöhe:

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 11

Der Schutzbedarf richtet sich danach, wie intensiv eine missbräuchliche Verarbeitung personenbezogener Daten den Betroffenen in seinem wirtschaftlichen und/oder in seinem gesellschaftlichen Belangen beeinträchtigen kann.

Gering: Bei der Verarbeitung des Namens und der Kommunikationsdaten des Geschäftsführers und des Leiters der IT handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten lässt.

Hoch/Gravierend: Ein hoher Schaden kann entstehen, wenn personenbezogene Daten verarbeitet werden, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann.

Darunter fallen personenbezogene Daten besonderer Kategorien (z.B. Gesundheitsdaten), personenbezogene Daten die dem Berufsgeheimnis unterliegen, deren Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann sowie personenbezogene Daten, die für Zwecke des Profiling verwendet werden können, insbesondere zur Analyse oder Prognose von Aspekten bezgl. Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, den Aufenthaltsort oder Ortswechsel, soweit dies rechtliche Wirkung für die betroffene Person entfaltet, oder sie in ähnlicher Weise erheblich beeinträchtigt.

Es gibt eine Vielzahl an denkbaren Situationen, bei denen sich ein hohes Risiko manifestieren kann. So könnte Le Chat zur Korrektur und Benotung von Klausuren ebenso eingesetzt werden wie zur Feststellung von Förderbedarf. Die Erstellung einer Kostenberechnung für einen Fördermittelantrag kann sowohl interne finanzielle Aspekte beinhalten wie auch personenbezogene Daten von eingesetzten Mitarbeitenden. Informationen wie die über den Förderbedarf eines Teilnehmenden kann für den Betroffenen ebenso zu gesellschaftlichen Nachteilen führen wie die bloße Kenntnis davon, dass bei einem Mitarbeitenden eine Lohnpfändung vorliegt. Die Kenntnis der veranschlagten Kalkulationsposten kann zu erheblichen wirtschaftlichen Nachteilen führen. Sowohl die Eingabe personenbezogener und/ oder wirtschaftlich relevanter Daten als auch die Verarbeitung auf durch US-Firmen gehosteten Servern könnte - zu einem gravierenden Schaden führen.

III. Ermittlung von Gefährdungen/ Bedrohungen für die Verfahrenskomponenten

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 12

Bedrohungen werden anhand des Gefährdungskatalog des BSI - IT Grundschutzkompendium – ermittelt.

G 0.19 Offenlegung schützenswerter Informationen

Vertrauliche Daten und Informationen dürfen nur den zur Kenntnisnahme berechtigten Personen zugänglich sein.

Soweit Le Chat über den Mistral Cloud Service La Plateforme gehostet wird, zeigt ein Blick auf die Subunternehmer, dass die Cloud-Infrastruktur der US-amerikanischen Unternehmen Microsoft und Google genutzt werden. Laut Datenschutzerklärung hostet Microsoft in Schweden und Norwegen und Google in Irland und den USA. Das ist aber im Zusammenhang mit der Frage der Offenlegung schützenswerter Daten unerheblich, denn der US-Cloud Act erlaubt amerikanischen Behörden den Zugriff auf Daten, die bei US-Anbietern gespeichert werden, auch dann, wenn sich die Server physisch in der EU befinden. Bei Nutzung des Mistral Cloud Service kann es also bei Eingabe von personenbezogenen Daten zur Offenlegung dieser Daten an die amerikanischen Behörden kommen.

G 0.29 Verstoß gegen Gesetze oder Regelungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind (beispielsweise durch ein unzureichendes Sicherheitsmanagement oder unvollständigen Datenschutz), kann dies zu Verstößen gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern führen. Zu denken ist hier insbesondere an die Verträge mit der öffentlichen Hand, z.B. der Arbeitsagentur, der Rentenversicherer und ähnliches.

Der Umgang mit personenbezogenen Daten ist über eine Vielzahl von Vorschriften geregelt. Dazu gehören die DS-GVO, das Gesetz über den kirchlichen Datenschutz, das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze, aber auch eine Vielzahl bereichsspezifischer Regelungen wie z.B. dem Sozialdatenschutz nach den Sozialgesetzbüchern.

Die Geschäftsführung eines Unternehmens ist dazu verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Hierzu gehört auch die Beachtung anerkannter Sicherheitsmaßnahmen. Zu denken ist hier z.B. an das KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), GmbHG (Gesetz betreffend die Gesellschaften mit beschränkter Haftung) oder das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), aus denen sich zu Risikomanagement und Informationssicherheit entsprechende Handlungs- und

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 13

Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen.

Bei Verträgen mit der Arbeitsagentur, den Rentenversicherern u.a. ist es üblich, dass der Auftraggeber die Einhaltung bestimmter Sicherheitsstandards vertraglich verpflichtend vorschreibt. Ein Verstoß gegen die Vertragspflichten kann zur Vertragsauflösung bis hin zum Verlust der Geschäftsbeziehung führen.

G 0.36 Identitätsdiebstahl

Beim Identitätsdiebstahl täuscht ein Angreifer eine falsche Identität vor, er benutzt also Informationen über eine andere Person, um in deren Namen aufzutreten. Hierfür werden Daten wie beispielsweise Geburtsdatum, Anschrift, Kreditkarten- oder Kontonummern benutzt, um sich beispielsweise auf fremde Kosten bei einem Internet-Dienstleister anzumelden oder sich auf andere Weise zu bereichern. Identitätsdiebstahl führt häufig auch direkt oder indirekt zur Rufschädigung, aber verursacht auch einen hohen Zeitaufwand, um die Ursachen aufzuklären und negative Folgen für die Betroffenen abzuwenden.

Werden Daten von Teilnehmenden z.B. zur Erstellung eines Lebenslaufes gepromptet und die Daten werden zum Training der KI genutzt, stehen diese Daten danach auch zum Identitätsdiebstahl bereit.

G 0.38 Missbrauch personenbezogener Daten

Ein Missbrauch personenbezogener Daten kann auch dann vorliegen, wenn eine Institution personenbezogene Daten ohne Rechtsgrundlage oder Einwilligung unberechtigt weitergibt. Für die Eingabe personenbezogener Daten in ein LLM das die Daten dann u.a. zum eigenen Training nutzt ist keine Rechtsgrundlage vorhanden und kann auch nach dem momentanen Stand der Dinge nicht einfach eine Einwilligung des Betroffenen als Rechtsgrundlage genutzt werden.

IV. Bewertung der Eintrittswahrscheinlichkeit

Selten/Überschaubar: Als selten wird die Eintrittswahrscheinlichkeit beurteilt, wenn der Eintritt des Schadens möglich ist, die konkreten Umstände aber gegen eine solche Entwicklung sprechen und nicht zu erwarten ist, dass sich daran etwas ändert.

Hinsichtlich der Gefahr eines Identitätsdiebstahls hängt der Schadenseintritt nicht nur davon ab, dass ein Mitarbeitender fälschlicherweise personenbezogene Daten durch Le Chat verarbeiten lässt, sondern zudem davon, dass ein Identitätsdieb konkret nach personenbezogenen Daten einer bestimmten Person fragen muss. Hat der möglichen Identitätsdieb keine Information darüber, dass

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 14

personenbezogene Daten durch Le Chat verarbeitet wurde, ist die Wahrscheinlichkeit eines Schadenseintritts denkmöglich, aber selten.

Das gleiche gilt für die Gefahr, dass die Geschäftsleitung die notwendige Sorgfalt außeracht lässt und Geschäftsgeheimnisse in das KI-System eingibt. Zwar ist der Eintritt eines Schadens möglich, er hängt aber von dem Verhalten der leitenden Mitarbeitenden ab, bei denen die Anzahl gering ist und man unterstellen darf, dass sie sich der Gefahr bewusst sind und von sich auch einem Schadenseintritt entgegenwirken.

Auch die reine Kenntnis der Kommunikationsdaten der Geschäftsführerin bzw. des Leiters der IT führen wahrscheinlich nicht zum Eintritt eines Schadens.

Gelegentlich/ Gravierend: Die Eintrittswahrscheinlichkeit wird als gelegentlich bewertet, wenn der Eintritt des Schadens möglich ist, aber von einem Verhalten Dritter abhängt, das sich nicht vorhersagen lässt.

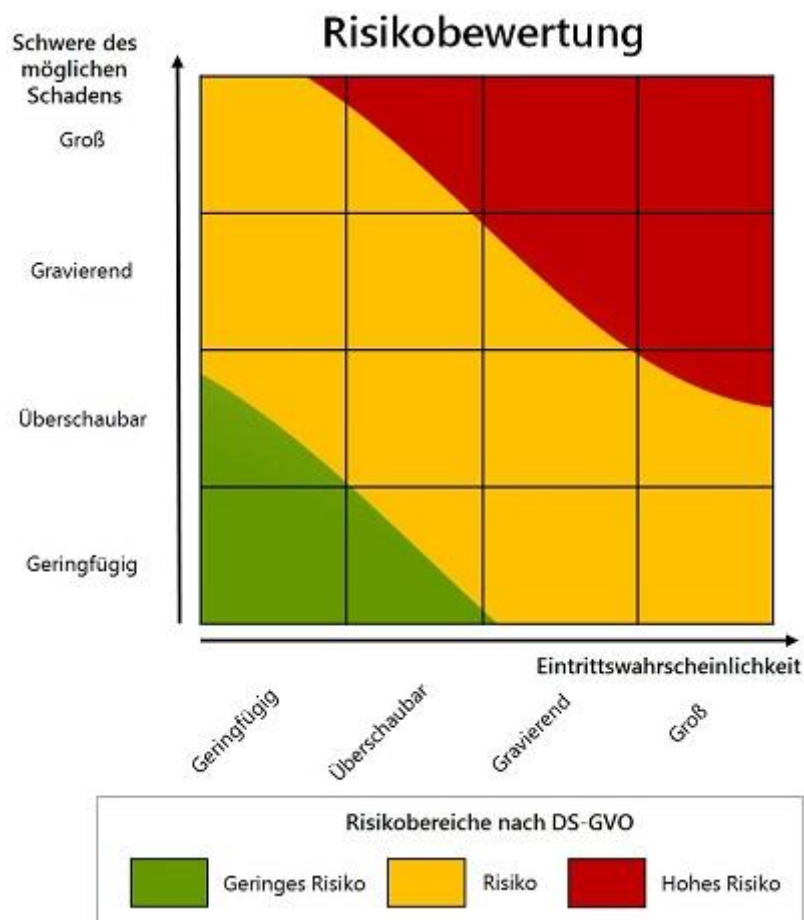
Das Risiko ist u.a. abhängig von der Zahl der Nutzer. Bewegt sich die Anzahl in einem hohen zweistelligen, vielleicht auch im dreistelligen Bereich, ist eine Anzahl von Personen erreicht, bei der sich nicht vorhersagen lässt, ob sich alle Mitarbeitenden zu jeder Zeit der Risiken der Eingabe von personenbezogenen Daten und/oder Geschäftsgeheimnissen bewusst sind, bzw. versehentlich solche Daten eingibt. Je mehr Menschen das System benutzen umso höher das Risiko des fehlerhaften Umgangs.

Zur Verarbeitung von Daten über die bei Microsoft und Google gehosteten Plattform La Plateforme bleibt festzustellen, dass sich auch hier der Schadenseintritt nicht vorhersagen lässt. In den USA befindet sich der Datenschutz im freien Fall. Nachdem einem Tech-Milliardär für drei Monate der freie Zugriff auf sämtliche IT der Regierung gewährt wurde ist nicht davon auszugehen, dass Daten, die durch amerikanische Unternehmen gehostet werden, vor einem Zugriff Dritter (Regierungsbehörden, Elon Musk, IT-Unternehmen) sicher sind. Hierfür spricht auch, dass die Federal Trade Commission (FTC), die als Behörde in den USA für Recht und Ordnung im Digitalraum sorgen soll, im August 2025 die 14 größten Tech-Unternehmen in den USA dazu aufforderte den Digital Service Act (EU-Gesetz) nicht zu befolgen, wenn amerikanische Interessen dagegen +stehen. Es spricht sehr viel dafür, dass die FTC eine vergleichbare Einstellung zur DSGVO hat. Bei Anwendung des Patriot Acts müssen US-Unternehmen den US-Behörden im Verdachtsfall Zugriff auf ihre Rechenzentren gewähren – unabhängig davon, wo sich diese Zentren

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 15

rein physisch befinden. Angesichts des unberechenbaren Verhaltens des amtierenden US-Präsidenten kann ein Verdachtsfall sehr schnell konstruiert sein. Laut der Nachrichtenagentur Reuters soll der amerikanische Präsident jüngst verschiedene Gesetze, die zur Regulierung und zum Datenschutz von den Vorgängerregierungen in Kraft gesetzt wurden, abgeschafft haben.

Bewertung: Geringer bis gravierender Schaden bei seltener bis gravierender Eintrittswahrscheinlichkeit



V. Auswertung:

Für einen Vertrauensvorschuss sorgt die Tatsache, dass ein zentrales Merkmal von Mistral AI die Transparenz ist. Die Kernmodelle wie Mistral 7B und Mistral 8x7B wurden als Open-Source-Projekte veröffentlicht. Auch das erkennbare Bemühen um DS-GVO Konformität z.B. die US-amerikanischen Subunternehmer nicht unterschlagen werden, ist positiv zu werten. Der Firmensitz in Frankreich hat zudem zur Konsequenz, dass Mistral AI bei der Entwicklung von Le Chat an die Vorgaben der DS-GVO gebunden ist. Anders als einige amerikanische Unternehmen schließt Mistral AI einen Auftragsdatenverarbeitungsvertrag mit den Kunden ab, wenn die Daten über La

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 16

Plattformen gehostet werden. Das Gewährleistungsziel der Transparenz ist durch die umfangreichen Informationen, die Mistral AI nicht nur zum Datenschutz allgemein, sondern auch zur Funktionsweise der Produkte zur Verfügung stellt, gewährleistet.

Hinsichtlich der Gewährleistungsziele der Vertraulichkeit und der Nichtverkettung stellen die oben genannten Fälle, bei denen mit einer geringen Eintrittswahrscheinlichkeit nur ein geringer Schaden entstehen kann, ein so niedriges Risiko dar, dass sie an dieser Stelle nicht weiter von Belang sind.

Die Antwort auf die Frage, ob sich die anderen oben benannten Risiken der Vertraulichkeit und der Nichtverkettung so begrenzen lassen, dass von einer datenschutzkonformen Anwendung von Le Chat über die unternehmenseigenen Plattform La Plateforme auszugehen ist, konzentriert sich hier auf zwei Bereiche.

Risiko der Eingabe personenbezogener Daten:

Zum einen stellt sich die Frage wie bei versehentlicher oder auch beabsichtigter Eingabe personenbezogener (oder auch wirtschaftlich relevanter) Daten ein hoher Schaden für den Betroffenen vermeiden lässt.

Hier kommen mehrere Maßnahmen – kumulativ, nicht alternativ - in Betracht.

1) Zu Beginn sollte eine Sensibilisierung der Mitarbeitenden durch eine entsprechende Schulung, die gem. Art. 4 KI-Verordnung sowieso vorgeschrieben ist, erfolgen. Hierbei sollte ausdrücklich darauf hingewiesen werden, dass personenbezogene Daten NICHT gepromptet werden dürfen. Die Frage, ob man mit einer Einwilligung des Betroffenen ausnahmsweise auch solche Daten eingeben darf, stellt sich jedenfalls dann erst einmal nicht, wenn öffentliche Institutionen (z.B.

Arbeitsagentur) vertraglich auf die Besonderheiten des Sozialdatenschutzes hingewiesen haben. Eine Differenzierung kann, nach Rücksprache mit den entsprechenden Auftraggebern, an strenge interne Regeln und auf jeden Fall auch an eine zuvor absolvierte, intensive Schulung mit Lernkontrolle gebunden sein.

2) Neben der Schulung sollte den Mitarbeitenden jederzeit Zugang zu einer Liste gewährt werden, in der dasjenige, das erlaubt ist, und dasjenige, was nicht erlaubt ist (Do and Do'nt Liste), aufgeführt sind.

3) Die Ein- und Ausgaben bei Le Chat werden bei der kostenlosen Variante zum Training der KI genutzt. Hierzu führt Mistral AI in der Datenschutzerklärung, Punkt 3 (siehe oben) aus:

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 17

Bitte beachten Sie, dass wir Ihren Input und Output nicht verwenden, um unsere Modelle für künstliche Intelligenz zu schulen, wenn Sie Le Chat Team, Le Chat Enterprise oder die kostenpflichtige Version unserer APIs verwenden. Wenn Sie einen Drittanbieter-Dienst mit den Mistral AI-Produkten verbinden, verwenden wir diesen Drittanbieterdienst nicht, um unsere Modelle der künstlichen Intelligenz zu schulen.

Die mit Abstand am häufigsten auftretende Datenschutzpanne ist die versehentlichen Fehlsendung von E-Mails. Angesichts dieser Erfahrungen ist zu erwarten, dass es auch zu einer versehentlichen Eingabe von personenbezogenen Daten in Le Chat kommen wird. Es ist daher erforderlich eine der aufgeführten Bezahlvarianten von Le Chat zu verwenden, um sicher zu stellen, dass selbst bei irrtümlicher Eingabe von personenbezogenen Daten oder Geschäftsgeheimnissen der Input und der Output nicht an die Öffentlichkeit gelangen. Anders als durch die vertragliche Zusicherung das die Daten nicht zum Training benutzt werden, kann man zumindest dem Sozialdatenschutz nicht gerecht werden.

4) Momentan wird weltweit intensiv daran gearbeitet Filter zu entwickeln, die personenbezogene Daten erkennen und ggfls. nicht verarbeiten. Das Thema sollte bei zuständigen Mitarbeitenden alle 6 Monate auf Wiedervorlage gelegt werden, um die Entwicklungen im Auge zu behalten und ggfls. dann zusätzliche Sicherheit durch Einrichtung eines entsprechenden Filters zu bekommen.

Risiko der Nutzung von La Plateforme:

Über La Plateforme können Unternehmen Mistral-Modelle per API in die eigenen Systeme integrieren. La Plateforme ist zum größten Teil in der EU gehostet, allerdings auf Servern, die sich zwar physisch in der EU befinden (Irland, Schweden und Norwegen), aber US-amerikanischen Tech-Unternehmen gehören. Es liegen – wie oben ausgeführt – hinreichende Indizien dafür vor, dass die amerikanischen Behörden durch Anwendung verschiedener amerikanischer Gesetze (Cloud Act, Patriot Pact etc.) Zugriff auf die in Europa gehosteten Daten nehmen könnten.

Grundsätzlich muss dann, wenn es zu einem Datenfluss in ein Drittland kommen kann, geprüft werden, ob in diesem Drittland – hier die USA –, ein mit der EU vergleichbarer Datenschutzstandard gewährleistet ist. Bislang sind verschiedene Vereinbarungen der EU mit den USA vom europäischen Gerichtshof (EuGH) jeweils als nicht ausreichend und damit rechtswidrig verworfen worden. Gegen den aktuellen Data Privacy Framework (DPF) und den dementsprechenden Angemessenheitsbeschluss der EU ist die Klage vor dem europäischen Gericht in erster Instanz abgelehnt worden. Hiergegen wird aller Voraussicht nach Beschwerde beim EuGH

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 18

erhoben werden, die nach Auffassung vieler Datenschutzexperten Aussicht auf Erfolg hat. Unabhängig davon gilt der Angemessenheitsbeschluss nur für die US-Unternehmen, die auf der offiziellen Liste zum EU-US DPF beim US-Handelsministerium mit einer aktiven Zertifizierung aufgeführt sind. Dies trifft zwar für Google, Microsoft und Stripe zu, allerdings nicht für die ebenfalls in den USA Daten verarbeitenden Unternehmen Blackforest Labs, Brave und Merge.dev zu. (Abruf 17.09.2025).

Mistral AI – offensichtlich um eine DS-GVO konforme Lösung bemüht – ist diesem Problem dadurch entgegengetreten, dass sie durch Abschluss der Standardvertragsklauseln den Datenschutz sichern wollten. Unter den bis zum Beginn des Jahres 2025 herrschenden Umständen wäre dieses Vorgehen als ausreichende Maßnahme zum Datenschutz zu bewerten gewesen.

Seit dem Amtsantritt des amtierenden US-Präsidenten findet auf der einen Seite eine kontinuierliche Abschaffung des Datenschutzes in den USA statt, während es auf der anderen Seite noch dazu durch die Abteilung für Regierungseffizienz (DOGE) zu unkontrollierten Zugriffen von Tech-Milliardären auf sämtliche amerikanischen staatlichen IT-Systeme kommt. Dass die FTC im August die großen Tech-Unternehmen dazu aufforderte, EU-Gesetze zu ignorieren, falls sie den amerikanischen Interessen widersprächen, macht deutlich, dass eine Vereinbarung von Mistral AI und den US- amerikanischen Unternehmen über die Standardvertragsklauseln kein Garant dafür ist, dass der europäischen Datenschutzstandard auch tatsächlich gewährt wird.

Hier bieten sich zwei Lösungsansätze an.

1) Zum einen bietet Mistral AI neben den allgemeinen AGB noch folgende Sondervereinbarung:

Sondervereinbarungen zu La Plateforme:

Ihre Nutzung von La Plateforme unterliegt unseren Nutzungsbedingungen und diesen zusätzlichen Bedingungen für La Plateforme.

Null Datenspeicherung. *Kunden können aus legitimen Gründen keine Vorratsdatenspeicherung verlangen. Mit dieser Option werden Ihr Ein- und Ausgang nur so lange verarbeitet, wie es zur Erzeugung des Outputs erforderlich ist, und werden nicht weiter aufbewahrt, es sei denn, es wird gesetzlich vorgeschrieben. Um Null-Datenspeicherung zu aktivieren, müssen Sie Ihre Anfrage über unser Hilfezentrum (verfügbar auf Ihrem Konto) oder Support-mistral.ai einreichen. Im Rahmen dieser Anfrage müssen Sie ausreichende Angaben zu Ihren berechtigten Gründen für die Erlangung*

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 19

von Null-Datenspeichern anfertigen. Wir werden Ihren Antrag prüfen und nach eigenem Ermessen den Antrag genehmigen oder ablehnen.

Inwieweit das – z.B. unter Hinweis auf den nur noch eingeschränkten Datenschutz in den USA vs. den strengen Sozialdatenschutz in Deutschland – zu einem positiven Ergebnis führt hängt allerdings von Mistral AI ab.

2) Zum anderen bietet Mistral AI an, das die Kunden ihre Daten selbst hosten können, bzw. ein Drittunternehmen damit beauftragen können den Datenfluss von Le Chat auf sicheren Server zu hosten. Aus rechtlicher Sicht ist eine Möglichkeit Le Chat ohne die Nutzung der Server von Microsoft und Google – mithin also wohl ohne Nutzung von La Plateforme - zu etablieren deutlich zu bevorzugen.

Vielleicht eröffnen sich zukünftig auch noch andere Wege, um La Plateforme datenschutzkonform zu nutzen. Welche Möglichkeit auch immer bevorzugt wird, zum jetzigen Zeitpunkt stellt die Nutzung von La Plateforme ohne Sicherstellung, dass keine US-amerikanisches Unternehmen involviert sind, ein nicht einschätzbares Risiko dar.

Abschließend bleibt Folgendes festzustellen

Mistral AI gibt sich deutlich Mühe die datenschutzkonforme Alternative zu Chat GPT, Claude u.a. zu sein. Das gelingt auch in weiten Teilen, weshalb diese Datenschutzfolgeabschätzung letztlich nur zwei Problembereiche thematisiert. Andere datenschutzrechtliche Anforderungen, wie z.B. Transparenz bezüglich der Löschung von Daten, Anonymisierung, Datenminimierung usw. werden von Vorneherein von Mistral AI erfüllt.

Soweit es gelingt die Beiden oben angesprochenen Problembereiche rechtlich korrekt in den Griff zu bekommen ist – Stand September 2025 - davon auszugehen, dass der Einsatz von Le Chat datenschutzkonform möglich ist. Inwieweit dies auch bei La Plateforme gelingen kann, hängt von der Antwort ab, die seitens Mistral AI z.B. zur Frage von „Null Datenspeicherung“ gegeben wird. Bei einer nicht zufriedenstellenden Antwort wäre die Alternative Le Chat zu nutzen und die anfallenden Daten durch ein europäisches Unternehmen in Europa datenschutzkonform zu hosten.

Zu guter Letzt:

Die Einführung einer datenschutzkonformen generativen KI ist ein dynamischer Prozess. Diese Datenschutzfolgeabschätzung basiert auf den Angaben von Mistral AI zum Zeitpunkt Juli 2025.

Analyse gem. RL zur Risikoanalyse und Risikobehandlung im Rahmen des KDM - Seite 20

Sollte es zu einem Einsatz von Mistral AI kommen, ist es ratsam bei jeder Mitteilung über die Veränderung der Verträge oder der Datenschutzbedingungen erneut zu prüfen, ob die Veränderung auch zu einer veränderten Risikoeinschätzung führt. Zudem sollte das Thema Datenschutz bei der generativen KI jährlich auf Wiedervorlage gelegt werden, um zu gewährleisten, dass eventuelle Veränderungen den Datenschutz nicht beeinträchtigen.