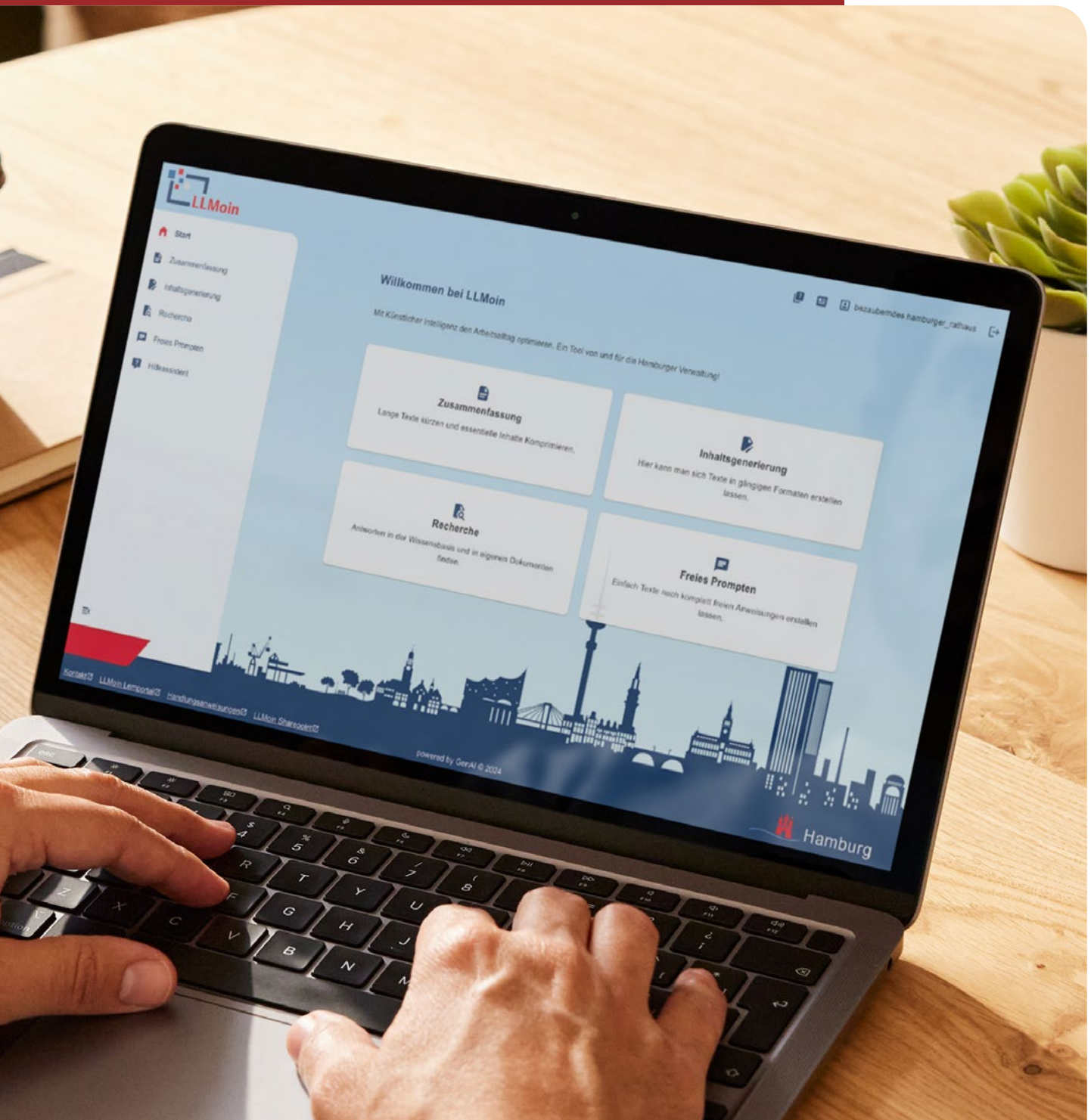




LLMoin

FAQ



Inhaltsverzeichnis

1. Überblick zu LLMoin	4
Was ist LLMoin?	4
Für wen ist LLMoin gedacht?	4
Welche typischen Anwendungsfälle gibt es für LLMoin?	4
Ersetzt LLMoin Mitarbeitende?	4
Wie unterscheidet sich LLMoin von frei verfügbaren KI-Diensten?	4
Wer betreibt LLMoin?	5
Kann jede Behörde LLMoin nutzen?	5
Ist LLMoin produktiv nutzbar oder nur ein Testsystem?	5
Gibt es Schulungen oder unterstützende Materialien zu LLMoin?	5
Welche Verantwortung haben Nutzende beim Einsatz von LLMoin?	5
2. Nutzung, Betrieb und Organisation	6
Wie erfolgt der Zugang zu LLMoin?	6
Gibt es eine Begrenzung der Nutzung (z. B. Anfragen, Volumen)?	6
Kann LLMoin produktiv in Fachverfahren eingesetzt werden?	6
Ist LLMoin für den Einsatz im Regelbetrieb geeignet?	6
Wer ist für den fachlichen Betrieb verantwortlich?	6
Wie wird mit fehlerhaften oder unzutreffenden Antworten umgegangen?	6
Kann LLMoin ohne Schulung genutzt werden?	7
Gibt es Nutzungsrichtlinien für LLMoin?	7
Welche Daten dürfen in LLMoin eingegeben werden?	7
Ist eine Nachnutzung von Ergebnissen aus LLMoin erlaubt?	7
Wie werden neue Anforderungen oder Fragen zu LLMoin adressiert?	7
3. Technik und Architektur	7
Auf welcher technischen Grundlage basiert LLMoin?	7
Wo wird LLMoin betrieben?	8
Werden die eingegebenen Daten zum Training der Modelle verwendet?	8
Welche Modelle kommen bei LLMoin zum Einsatz?	8
Ist LLMoin mandantenfähig?	8
Wie wird die Verfügbarkeit von LLMoin sichergestellt?	8
Gibt es eine Protokollierung oder ein Logging der Nutzung?	8
Kann LLMoin in bestehende IT-Landschaften integriert werden?	8
Ist LLMoin skalierbar?	8
Wie wird mit Updates oder Modelländerungen umgegangen?	8

4. Datenschutz und Informationssicherheit	9
Ist LLMoin datenschutzkonform nutzbar?	9
Welche datenschutzrechtliche Rolle hat Dataport bei LLMoin?	9
Wer ist für die Datenschutzbewertung (z. B. DSFA) verantwortlich?	9
Welche Schutzbedarfseinstufung hat LLMoin?	9
Dürfen personenbezogene Daten in LLMoin verarbeitet werden?	9
Werden Inhalte oder Eingaben dauerhaft gespeichert?	9
Wer hat Zugriff auf die eingegebenen Inhalte?	10
Werden Daten an externe Anbieter oder ins Ausland übermittelt?	10
Wie wird die Informationssicherheit gewährleistet?	10
Ist LLMoin für vertrauliche oder geheime Informationen geeignet?	10
5. API, Schnittstellen und technische Anbindung	10
Gibt es eine API für LLMoin?	10
Für welche Anwendungsfälle ist die API gedacht?	10
Wie erfolgt der Zugriff auf die LLMoin-API?	11
Ist die Nutzung der API auch produktiv möglich?	11
Gibt es technische Dokumentationen zur API?	11
Können eigene Datenquellen angebunden werden?	11
Wer ist für die Umsetzung der Schnittstellenanbindung verantwortlich?	11
Gibt es Einschränkungen bei der API-Nutzung?	11
Wie wird die Sicherheit bei der API-Nutzung gewährleistet?	11
6. Recht, Vertrag, Nachnutzung und Sonstiges	12
Auf welcher rechtlichen Grundlage wird LLMoin bereitgestellt?	12
Gibt es einen separaten Vertrag für LLMoin?	12
Wie ist die Haftung für Ergebnisse aus LLMoin geregelt?	12
Dürfen die mit LLMoin erzeugten Inhalte weiterverwendet werden?	12
Gibt es Einschränkungen bei der Nachnutzung der Ergebnisse?	12
Wer ist Urheber der mit LLMoin erzeugten Inhalte?	12
Kann LLMoin auch für externe Veröffentlichungen genutzt werden?	13
Wie wird mit Feedback, Fehlern oder Verbesserungsvorschlägen umgegangen?	13
Gibt es besondere Einschränkungen oder Ausschlüsse bei der Nutzung?	13

1. Überblick zu LLMoin



Was ist LLMoin?

LLMoin ist ein generatives Sprachmodell-Angebot von Dataport, das Verwaltungen beim Beantworten von Fragen, bei Textentwürfen, Analysen und Wissensarbeit unterstützt. Es basiert auf Large Language Models (LLMs) und wird in einer datenschutz- und sicherheitskonformen Umgebung betrieben.



Für wen ist LLMoin gedacht?

LLMoin richtet sich primär an öffentliche Verwaltungen, Behörden und öffentliche Unternehmen, die generative KI sicher und kontrolliert einsetzen möchten.



Welche typischen Anwendungsfälle gibt es für LLMoin?

Typische Einsatzszenarien sind:

- Unterstützung bei der Texterstellung (z. B. Entwürfe, Zusammenfassungen)
- Beantwortung fachlicher Fragen auf Basis bereitgestellter Inhalte
- Analyse und Strukturierung von Texten
- Unterstützung bei Recherche- und Wissensaufgaben

LLMoin ist ausdrücklich kein System zur automatisierten Entscheidungsfindung.



Ersetzt LLMoin Mitarbeitende?

Nein. LLMoin ist als Assistenzsystem konzipiert. Die fachliche Verantwortung, Prüfung und Freigabe der Ergebnisse liegen immer bei den Nutzenden.



Wie unterscheidet sich LLMoin von frei verfügbaren KI-Diensten?

Im Gegensatz zu frei zugänglichen KI-Diensten:

- wird LLMoin in einer kontrollierten, behördentauglichen Umgebung betrieben,
- werden keine Eingaben zum Training öffentlicher Modelle verwendet,
- gelten klare Regelungen zu Datenschutz, Sicherheit und Betrieb,
- erfolgt die Nutzung im Rahmen vertraglich geregelter Bedingungen.



Wer betreibt LLMoin?

LLMoin wird von Dataport betrieben.



Kann jede Behörde LLMoin nutzen?

Grundsätzlich ja, sofern die organisatorischen, rechtlichen und technischen Voraussetzungen erfüllt sind. Die konkrete Nutzung erfolgt projekt- bzw. kundenbezogen und kann Abstimmungen (z.B. Datenschutz, IT-Sicherheit) erfordern.



Ist LLMoin produktiv nutzbar oder nur ein Testsystem?

LLMoin kann sowohl zu Test- und Erprobungszwecken als auch produktiv eingesetzt werden. Art und Umfang der Nutzung hängen vom jeweiligen Nutzungsszenario und den getroffenen Vereinbarungen ab.



Gibt es Schulungen oder unterstützende Materialien zu LLMoin?

Ja. Es stehen Richtlinien, Leitfäden, Schulungs- und Informationsmaterialien zur Verfügung, die den sicheren und sinnvollen Einsatz von LLMoin unterstützen.



Welche Verantwortung haben Nutzende beim Einsatz von LLMoin?

Nutzende sind verantwortlich für:

- die inhaltliche Prüfung der Ergebnisse,
- die Einhaltung geltender Vorgaben (z.B. Datenschutz, Geheimhaltung),
- die sachgerechte Nutzung entsprechend der bereitgestellten Leitlinien.

2. Nutzung, Betrieb und Organisation



Wie erfolgt der Zugang zu LLMoin?

Der Zugang zu LLMoin erfolgt über bereitgestellte Benutzerkonten. Diese werden projekt- bzw. kundenbezogen eingerichtet und verwaltet. Testzugänge sind möglich.



Gibt es eine Begrenzung der Nutzung (z. B. Anfragen, Volumen)?

Ja. Die Nutzung kann durch technische oder vertragliche Rahmenbedingungen begrenzt sein (z.B. Anzahl der Anfragen, Nutzungsdauer, Testzeiträume). Die konkreten Limits hängen vom jeweiligen Nutzungsszenario ab.



Kann LLMoin produktiv in Fachverfahren eingesetzt werden?

Ja, grundsätzlich ist eine produktive Nutzung möglich. Voraussetzung ist, dass:

- das Einsatzszenario fachlich geeignet ist,
- Datenschutz- und Sicherheitsanforderungen erfüllt sind,
- eine entsprechende Abstimmung mit Dataport erfolgt ist.



Ist LLMoin für den Einsatz im Regelbetrieb geeignet?

LLMoin kann in den Regelbetrieb überführt werden, sofern die organisatorischen, technischen und rechtlichen Voraussetzungen erfüllt sind und der Einsatz zuvor geprüft wurde.



Wer ist für den fachlichen Betrieb verantwortlich?

Die fachliche Verantwortung für Inhalte und Ergebnisse liegt immer bei der nutzenden Organisation bzw. den Mitarbeitenden. Dataport stellt den technischen Betrieb bereit.



Wie wird mit fehlerhaften oder unzutreffenden Antworten umgegangen?

Antworten von LLMoin sind stets zu prüfen. Fehlerhafte oder unzutreffende Ergebnisse müssen von den Nutzenden erkannt und korrigiert werden. LLMoin liefert Vorschläge, keine verbindlichen Aussagen.



Kann LLMoin ohne Schulung genutzt werden?

Grundsätzlich ja, empfohlen wird jedoch dringend die Nutzung der bereitgestellten Leitfäden, Richtlinien und Schulungsmaterialien, um Fehlanwendungen zu vermeiden.



Gibt es Nutzungsrichtlinien für LLMoin?

Ja. Für LLMoin existieren Nutzungsrichtlinien und Leitfäden, die u. a. den zulässigen Einsatz, den Umgang mit sensiblen Daten und die Verantwortung der Nutzenden regeln.



Welche Daten dürfen in LLMoin eingegeben werden?

Es dürfen nur Daten eingegeben werden, deren Verarbeitung zulässig ist. Insbesondere sind personenbezogene, vertrauliche oder schutzbedürftige Informationen nur entsprechend der geltenden Vorgaben und Freigaben zu verwenden.



Ist eine Nachnutzung von Ergebnissen aus LLMoin erlaubt?

Ja, die Ergebnisse können grundsätzlich weiterverwendet werden. Die Verantwortung für Inhalt, Korrektheit und rechtliche Zulässigkeit liegt jedoch bei den Nutzenden.



Wie werden neue Anforderungen oder Fragen zu LLMoin adressiert?

Anforderungen, Rückfragen oder Erweiterungswünsche werden über die bekannten Kontakt- und Supportwege an Dataport herangetragen und geprüft.

3. Technik und Architektur



Auf welcher technischen Grundlage basiert LLMoin?

LLMoin basiert auf Large Language Models (LLMs), die über eine von Dataport betriebene Plattform bereitgestellt werden. Die technische Umsetzung ist so gestaltet, dass sie den Anforderungen öffentlicher Verwaltungen entspricht.



Wo wird LLMoin betrieben?

LLMoin wird in einer von Dataport kontrollierten Infrastruktur betrieben. Der Betrieb erfolgt nicht in einer frei zugänglichen öffentlichen Cloud.



Werden die eingegebenen Daten zum Training der Modelle verwendet?

Nein. Eingaben und Inhalte werden nicht zum Training öffentlich zugänglicher Modelle verwendet. Die Nutzung der Daten erfolgt ausschließlich zur Bearbeitung der jeweiligen Anfrage.



Welche Modelle kommen bei LLMoin zum Einsatz?

Bei LLMoin kommen verschiedene Sprachmodelle zum Einsatz. Die konkrete Modellauswahl kann sich im Laufe der Zeit ändern und wird von Dataport gesteuert.



Ist LLMoin mandantenfähig?

Ja. LLMoin ist mandantenfähig, sodass Daten und Nutzungen verschiedener Organisationen voneinander getrennt sind.



Wie wird die Verfügbarkeit von LLMoin sichergestellt?

Die Verfügbarkeit wird im Rahmen des technischen Betriebs durch Dataport sichergestellt. Details zu Verfügbarkeiten und Servicezeiten ergeben sich aus den jeweiligen Vereinbarungen.



Gibt es eine Protokollierung oder ein Logging der Nutzung?

Ja. Es findet eine technisch notwendige Protokollierung statt, z.B. zu Betriebs- und Sicherheitszwecken. Inhalte werden nicht ohne Zweck verarbeitet.



Kann LLMoin in bestehende IT-Landschaften integriert werden?

Ja. LLMoin kann in bestehende IT-Landschaften eingebunden werden, z.B. über Schnittstellen oder organisatorisch eingebettete Nutzungsszenarien.



Ist LLMoin skalierbar?

Ja. Die Plattform ist so ausgelegt, dass sie skalierbar betrieben werden kann, abhängig von Nutzungsszenarien und vereinbarten Rahmenbedingungen.



Wie wird mit Updates oder Modelländerungen umgegangen?

Updates und Änderungen an der technischen Plattform oder den Modellen erfolgen kontrolliert durch Dataport. Ziel ist es, Funktionalität, Sicherheit und Qualität kontinuierlich zu verbessern.

4. Datenschutz und Informationssicherheit



Ist LLMoin datenschutzkonform nutzbar?

Ja. LLMoin ist so konzipiert, dass eine datenschutzkonforme Nutzung möglich ist. Voraussetzung ist, dass die nutzende Organisation die geltenden Datenschutzvorgaben einhält und LLMoin entsprechend der bereitgestellten Richtlinien einsetzt.



Welche datenschutzrechtliche Rolle hat Dataport bei LLMoin?

Dataport tritt im Rahmen von LLMoin in der Regel als Auftragsverarbeiter auf. Die Verantwortung für die rechtmäßige Verarbeitung der Inhalte liegt bei der nutzenden Stelle.



Wer ist für die Datenschutzbewertung (z. B. DSFA) verantwortlich?

Die Durchführung und Bewertung einer Datenschutz-Folgenabschätzung (DSFA) liegt in der Verantwortung der nutzenden Organisation. Dataport stellt hierfür unterstützende Informationen bereit.



Welche Schutzbedarfseinstufung hat LLMoin?

Für LLMoin wurde eine Schutzbedarfseinstufung vorgenommen. Die konkrete Einstufung und Begründung kann von Dataport zur Verfügung gestellt werden und dient als Grundlage für die Bewertung durch die nutzenden Stellen.



Dürfen personenbezogene Daten in LLMoin verarbeitet werden?

Personenbezogene Daten dürfen nur im Rahmen der geltenden rechtlichen Vorgaben und unter Beachtung der bereitgestellten Richtlinien verarbeitet werden. In vielen Szenarien wird empfohlen, auf die Eingabe personenbezogener Daten zu verzichten oder diese zu anonymisieren.



Werden Inhalte oder Eingaben dauerhaft gespeichert?

Eingaben werden nicht dauerhaft für Trainingszwecke gespeichert. Eine Speicherung erfolgt nur, soweit sie für den technischen Betrieb, die Sicherheit oder vereinbarte Zwecke erforderlich ist.



Wer hat Zugriff auf die eingegebenen Inhalte?

Zugriff auf Inhalte haben nur berechnigte Stellen im Rahmen des Betriebs. Eine Weitergabe an Dritte oder Nutzung für fremde Zwecke erfolgt nicht.



Werden Daten an externe Anbieter oder ins Ausland übermittle?

Nein. LLMoin wird in einer kontrollierten Umgebung betrieben. Eine unkontrollierte Übermittlung von Daten an externe Anbieter oder in Drittstaaten findet nicht statt.



Wie wird die Informationssicherheit gewährleitet?

Die Informationssicherheit wird durch technische und organisatorische Maßnahmen sichergestellt, die den Anforderungen an den Betrieb in der öffentlichen Verwaltung entsprechen.



Ist LLMoin für vertrauliche oder geheime Informationen geeignet?

Der Umgang mit vertraulichen oder besonders schutzbedürftigen Informationen ist nur im Rahmen der geltenden Vorgaben zulässig. Ob und in welchem Umfang solche Daten verarbeitet werden dürfen, ist durch die nutzende Organisation zu bewerten.

5. API, Schnittstellen und technische Anbindung



Gibt es eine API für LLMoin?

Ja. LLMoin stellt eine API zur Verfügung, über die das Sprachmodell in eigene Anwendungen oder Fachverfahren eingebunden werden kann.



Für welche Anwendungsfälle ist die API gedacht?

Die API ist insbesondere für:

- die Integration in Fachverfahren,
- die Nutzung in eigenen Anwendungen,

– automatisierte oder teilautomatisierte Workflows
geeignet, sofern die fachlichen und rechtlichen Voraussetzungen erfüllt sind.



Wie erfolgt der Zugriff auf die LLMoin-API?

Der Zugriff erfolgt über authentifizierte Schnittstellen. Die konkreten Zugangsdaten und technischen Details werden im Rahmen der jeweiligen Vereinbarung bereitgestellt.



Ist die Nutzung der API auch produktiv möglich?

Ja. Die API kann sowohl zu Testzwecken als auch produktiv genutzt werden, sofern das Nutzungsszenario abgestimmt und freigegeben ist.



Gibt es technische Dokumentationen zur API?

Ja. Für die API stehen technische Dokumentationen und Schnittstellenbeschreibungen zur Verfügung, die die Nutzung und Anbindung erläutern.



Können eigene Datenquellen angebunden werden?

Eine Anbindung eigener Datenquellen ist grundsätzlich möglich, z. B. im Rahmen spezifischer Integrationsszenarien. Die konkrete Umsetzung erfordert eine fachliche und technische Abstimmung.



Wer ist für die Umsetzung der Schnittstellenanbindung verantwortlich?

Die technische Umsetzung der Anbindung liegt in der Regel bei der nutzenden Organisation. Dataport unterstützt durch Bereitstellung der Schnittstellen und notwendiger Informationen.



Gibt es Einschränkungen bei der API-Nutzung?

Ja. Die API-Nutzung kann durch technische, sicherheitsrelevante oder vertragliche Vorgaben eingeschränkt sein, z. B. hinsichtlich Umfang, Zugriff oder Nutzungsszenarien.



Wie wird die Sicherheit bei der API-Nutzung gewährleistet?

Die Sicherheit wird durch Authentifizierungs- und Autorisierungsmechanismen sowie durch technische Schutzmaßnahmen sichergestellt.

6. Recht, Vertrag, Nachnutzung und Sonstiges



Auf welcher rechtlichen Grundlage wird LLMoin bereitgestellt?

Die Bereitstellung von LLMoin erfolgt auf Grundlage vertraglicher Vereinbarungen zwischen Dataport und der nutzenden Organisation. Die konkreten rechtlichen Rahmenbedingungen ergeben sich aus dem jeweiligen Vertrag.



Gibt es einen separaten Vertrag für LLMoin?

Ja. Die Nutzung von LLMoin wird über eigene vertragliche Regelungen abgebildet, z. B. im Rahmen bestehender Verträge oder ergänzender Vereinbarungen.



Wie ist die Haftung für Ergebnisse aus LLMoin geregelt?

Die Verantwortung für die Nutzung und Bewertung der Ergebnisse liegt bei der nutzenden Organisation. LLMoin liefert Unterstützung, aber keine rechtsverbindlichen oder fachlich geprüften Aussagen.



Dürfen die mit LLMoin erzeugten Inhalte weiterverwendet werden?

Ja. Die mit LLMoin erzeugten Inhalte dürfen grundsätzlich weiterverwendet werden. Die inhaltliche, fachliche und rechtliche Verantwortung liegt jedoch bei den Nutzenden.



Gibt es Einschränkungen bei der Nachnutzung der Ergebnisse?

Die Nachnutzung unterliegt den vertraglichen und rechtlichen Rahmenbedingungen. Insbesondere ist sicherzustellen, dass keine Schutzrechte Dritter verletzt werden.



Wer ist Urheber der mit LLMoin erzeugten Inhalte?

Die urheberrechtliche Einordnung hängt vom jeweiligen Nutzungsszenario ab. In der Praxis liegt die Verantwortung für die Nutzung der Inhalte bei der nutzenden Organisation.



Kann LLMoin auch für externe Veröffentlichungen genutzt werden?

Ja, grundsätzlich ist dies möglich. Inhalte müssen jedoch vor einer Veröffentlichung fachlich geprüft und freigegeben werden.



Wie wird mit Feedback, Fehlern oder Verbesserungsvorschlägen umgegangen?

Feedback und Verbesserungsvorschläge können über die bekannten Support- und Kontaktwege an Dataport gemeldet werden und fließen in die Weiterentwicklung ein.



Gibt es besondere Einschränkungen oder Ausschlüsse bei der Nutzung?

LLMoin darf nicht für unzulässige Zwecke oder entgegen geltender Vorgaben eingesetzt werden. Details ergeben sich aus den Nutzungsbedingungen und Richtlinien.