

# Freie und Hansestadt Hamburg

Senatskanzlei

**Datenschutzfolgenabschätzung nach Art. 35 DS-GVO**

25.07.2025

# Datenschutzfolgenabschätzung nach Art. 35 DS-GVO

Bezeichnung der Verarbeitungstätigkeit: Bereitstellung von LLMoin

## 1. Information zur Datenschutzfolgenabschätzung:

1.1	Name des Bearbeiters:	
1.2	Name des Datenschutzbeauftragten:	
1.3	Bearbeitungsdatum:	

## 2. Grundlegende Informationen:

2.1	Welche Verarbeitung ist geplant?  Hinweis: Grundlage der DSFA ist die systematische Beschreibung der Verarbeitungstätigkeit. Innovative Prozesse, erstmals beim Verantwortlichen genutzte technische Mittel und Besonderheiten, die mit der Verarbeitung verbunden sind, sollten dabei besonders erwähnt werden. Es bietet sich an, diese Beschreibung der Prozesse in einer Anlage darzustellen.	Siehe Ziffer 2.1 der Beschreibung der Verarbeitungstätigkeit LLMoin.
2.2	Welche Zuständigkeiten bestehen für die Verarbeitung?	Für die Bereitstellung von LLMoin ist die fachliche Leitstelle LLMoin zuständig. Datenschutzrechtlich verantwortlich ist SK/ITD. Dataport ist Auftragsverarbeiterin im Sinne des Art. 4 Nr. 8 DSGVO. Microsoft Corporation ist Unterauftragsverarbeiterin gemäß Art. 28 Abs. 2 DSGVO.
2.3	Gibt es Normen oder Standards für die Verarbeitung?	DSGVO, HmbDSG, HmbVwDiG, HmbStatG, KIVO.

## 3. Daten, Prozesse und Unterstützung

3.1	Welche Daten werden verarbeitet?  Hinweis: Optimalerweise werden hier in Form einer Auflistung auch die unterschiedlichen Kategorien von Daten voneinander abgegrenzt,	Metadaten.  Im Übrigen, d.h. in Bezug auf die Prompts, ist die Art der personenbezogenen Daten abhängig vom jeweiligen Verarbeitungskontext, in dem die Nutzung von LLMoin erfolgt.
-----	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	um die Einschätzung im Zuge der Schwellwertanalyse zu vereinfachen.	<p>Ausgenommen sind die Daten nach Art. 9 und 10 DSGVO, Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, sowie Personalakten, soweit sie vertrauliche oder höchstpersönliche Daten darstellen.</p> <p>Ausgenommen sind auch Daten aus der Wissensbasis von LLMoin, soweit sie von den dahinterstehenden Personen nicht veröffentlicht worden sind.</p>
3.2	Wie verläuft der Lebenszyklus von Daten und Prozessen?	<p>Alle Prompt-Inhalte werden 1. Von dem User eingegeben, 2. Von LLMoin umstrukturiert (LLMoin läuft auf Dataport Rechnern), 3. An Azure LLM Endpoints geschickt, 4. Die Antwort via LLMoin an den User gegeben.</p> <p>Die Prompts und Antworten von 2. und 3. Werden sofort nach der Erstellung bei Azure gelöscht.</p> <p>Die Speicherung der Daten in den verschiedenen Komponenten (Frontend, Backend und Azure) ist im Detail in der Tabelle 5.1 des Konzepts zur Datenspeicherung und Datenlöschung zu finden.</p> <p>Eine weitere Übersicht über den Datenfluss bietet das Kapitel 7.2 „Datenfluss“ aus dem Konzept zur Datenspeicherung und Datenlöschung.</p>
3.3	<p>Mit Hilfe welcher Mittel erfolgt die Datenverarbeitung?</p> <p>Hinweis: Die Datenflüsse zwischen den Komponenten sollten deutlich gemacht werden. Auch muss deutlich werden, welche Daten auf welchen Mitteln verarbeitet werden, um daraus in den weiteren Schritten spezifische Risiken und erforderliche Maßnahmen ableiten zu können.</p>	<p>Die Mittel und IT Stack, mit denen die Daten verarbeitet werden lässt sich auch an der oben erwähnten Tabelle (5.1 Übersicht: Datenspeicherung nach fachlicher Kategorie) ablesen.</p> <p>Die Komponenten sind zusammenfassend:</p> <ul style="list-style-type: none"> <li>- Opensearch</li> <li>- Prometheus</li> <li>- Azure System (Log)</li> <li>- Keycloak</li> <li>- Plattform K8s</li> <li>- Basis Dienst Container Infrastruktur</li> </ul>

4. Verhältnismäßigkeit und Notwendigkeit		
4.1	Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?	Ja.

4.2	<p>Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?</p> <p>Hinweis: Eine genaue Bezeichnung der Rechtsgrundlage unter Nennung der spezifischen für die Verarbeitungstätigkeit einschlägigen Paragraphen sollte an dieser Stelle aufgenommen werden.</p>	Siehe Ziffer 2.1 der Beschreibung der Verarbeitungstätigkeit LLMoin.
4.3	<p>Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?</p> <p>Hinweis: Hier sollte kurz, gerne stichpunktartig, dargelegt werden, weshalb jedes einzelne Datum für die Verarbeitung notwendig ist und ohne dieses Datum das gesetzte Ziel der Verarbeitung nicht erfüllt werden kann.</p>	Ja. Die Datenverarbeitungen erfolgen zu festgelegten Zwecken (Gewährleistung der Funktionalitäten zur Erledigung öffentlicher Aufgaben, Nutzerfreundlichkeit und -einstellungen, Sicherheit und ordnungsgemäßer Betrieb, Erfüllung von Betroffenenrechten, Anpassung der Nutzeroberfläche, Produktakzeptanzmessung und -verbesserung) und sind mit Blick auf die jeweils verfolgten Zwecke notwendig und verhältnismäßig.
4.4	Sind die Daten korrekt und auf dem neuesten Stand?	Ja.
4.5	Welche Speicherdauer haben die Daten?	Siehe Ziffer 5 der Beschreibung der Verarbeitungstätigkeit LLMoin.

<b>5. Maßnahmen zu Schutz der Persönlichkeitsrechte der betroffenen Personen</b>		
5.1	Wie werden die betroffenen Personen über die Verarbeitung informiert?	<p>Die Nutzenden von LLMoin, deren Daten verarbeitet werden, werden über Datenschutzhinweise informiert, die über das Browserfenster im Footer abrufbar sind.</p> <p>Die Bürger:innen, deren Daten in LLMoin verarbeitet werden können, werden über Datenschutzhinweise in den Eingangskanälen für behördliche Verwaltungsleistungen (OSI-Plattform) informiert.</p>
5.2	Wenn anwendbar: wie wird die Einwilligung der betroffenen Personen eingeholt?	Über die Nutzungsoberfläche durch Opt-In.
5.3	Wie können Betroffene ihre Rechte auf Auskunft und Datenübertragbarkeit ausüben?	<p>Soweit die Betroffenenrechte die</p> <ul style="list-style-type: none"> <li>- Erzeugung von Antworten auf Grundlage der Eingaben/Prompts in LLMoin betreffen,</li> <li>- Weiterverarbeitungen von Nutzungsdaten (Eingaben / Prompts, Antworten, Metadaten) sowie</li> <li>- Erzeugung von Ausgaben personenbezogener Daten aus der Wissensbasis von LLMoin</li> </ul>

		<p>betreffen, können Betroffene ihre Betroffenenrechte gegenüber der Fachlichen Leitstelle für LLMoin durch entsprechende Mitteilung (E-Mail, Brief) geltend machen. Datenschutzrechtliche Fragen können an den/die Datenschutzbeauftragte:n des Verantwortlichen gerichtet werden.</p> <p>Soweit die Betroffenenrechte die</p> <ul style="list-style-type: none"> <li>- Auswahl der Eingaben/Prompts in LLMoin und</li> <li>- die Weiterverwendung der Antworten zur Erledigung öffentlicher Aufgaben</li> </ul> <p>betreffen, können betroffene Nutzende von LLMoin sich an den/die für sie zuständige:n Datenschutzbeauftragte:n wenden. Betroffene Bürger:innen können sich an die Behörde wenden, mit der sie in Kontakt getreten sind.</p>
5.4	Wie können betroffene Personen ihre Rechte auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?	<p><b>a. Im KI-Modell:</b></p> <p>Die Durchsetzung von Berichtigung und Löschung von personenbezogenen Daten im KI-Modell von LLMoin wird umgesetzt durch Intent-Routing und den Abgleich mit einer (Black-)Liste, in der die zu berichtigenden und berichtigten Daten oder die zu löschenden Daten aufgeführt sind.</p> <p><b>b. Im Nutzungsdatensatz:</b></p> <p>Löschung von Chatverläufen kann in den Nutzereinstellungen vorgenommen werden.</p> <p>Löschung von Feedback mit Erläuterungen kann in den Nutzereinstellungen vorgenommen werden.</p> <p>Löschung individueller Konfigurationen und Einstellungen kann in den Nutzereinstellungen vorgenommen werden.</p> <p><b>c. Im Übrigen:</b></p> <p>Betroffene können Berichtigung und Löschung gegenüber der Fachlichen Leitstelle für LLMoin durch entsprechende Mitteilung (E-Mail, Brief) geltend machen.</p>
5.5	Wie können betroffene Personen ihre Rechte auf Einschränkung der Verarbeitung oder Widerspruch ausüben?	<p><b>a. Im KI-Modell:</b></p> <p>Die Durchsetzung von Einschränkung der Verarbeitung und Widerspruch gegen</p>

		<p>Datenverarbeitungen im KI-Modell von LLMoin wird umgesetzt durch Intent-Routing und den Abgleich mit einer (Black-)Liste, in der die zu blockierenden Daten aufgeführt sind.</p> <p><b>b. Im Nutzungsdatensatz:</b></p> <p>Einschränkung der Verarbeitung und Widerspruch gegen die Verwendung von Prompts kann durch Löschung von Chatverläufen in den Nutzereinstellungen vorgenommen werden.</p> <p>Einschränkung der Verarbeitung und Widerspruch gegen die Verwendung von Feedback mit Erläuterungen kann durch Löschung in den Nutzereinstellungen vorgenommen werden.</p> <p>Einschränkung der Verarbeitung und Widerspruch gegen die Umsetzung individueller Konfigurationen und Einstellungen kann durch Löschung in den Einstellungen vorgenommen werden.</p> <p><b>c. Im Übrigen:</b></p> <p>Im Übrigen können Betroffene Einschränkung der Verarbeitung und Widerspruch gegenüber der Fachlichen Leitstelle für LLMoin durch entsprechende Mitteilung (E-Mail, Brief) geltend machen.</p>
5.6	<p>Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?</p> <p>Hinweis: Vertragsunterlagen zur Anlage nehmen</p>	Ja.
5.7	<p>Soweit Datenübermittlungen in Länder außerhalb der EU stattfinden, werden die Daten angemessen geschützt?</p>	Ja.

## 6. Bestehende und ggf. geplante Maßnahmen

Hinweis: Zunächst werden die bestehenden Maßnahmen aufgeführt. Diese bestehenden Maßnahmen werden nach Risikobetrachtung erneut betrachtet und ggf. ergänzt und erweitert.

6.1	<p>Dokumentation</p> <p>Hinweis: Die Dokumentation sollte zur Anlage genommen werden.</p>	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
-----	-------------------------------------------------------------------------------------------	-------------------------------------------------------------------------

6.2	<b>Protokollierung</b>  Hinweis: Der Protokollierung ist spezifisch für die jeweils genutzten Komponenten zu benennen. Es muss insbesondere deutlich werden zu welchem Zweck die Protokolle erstellt werden, welche Prozesse protokolliert werden (lesende Zugriffe, schreibende Zugriffe) welche Merkmale protokolliert werden, wo die Protokolle gespeichert werden und wie lange, wer Zugriff auf die Protokolle hat und ob für die Nutzung der Protokolle spezifische Regelungen getroffen werden. Es bietet sich an, die Ausführungen in einer Anlage zu beschreiben.	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Siehe Ziffer 5.1 des Konzepts zur Datenspeicherung und Datenlöschung.
6.3	<b>Mandantentrennung</b>  Hinweis: Bei einer Mandantentrennung sollte insbesondere deutlich werden, zwischen welchen Mandanten unterschieden wird und durch welche technischen Maßnahmen die Mandantentrennung erfolgt (vgl. ggf. sollte hier ein Hinweis auf den Baustein Trennung des Standarddatenschutzmodells erfolgen).	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Eine Mandantentrennung entsteht durch das Rollen und Rechtekonzept, in der jeder User nur auf seine eigenen Daten und Chatverläufe Zugriff hat. Manche Daten, insbesondere die hinterlegten Datensätze bei der Recherche werden innerhalb einer Einrichtung (Behörden, Bezirke, u.ä.) geteilt aber nicht über diese Einrichtung hinaus.  Eine physische Trennung auf Ebene der Infrastruktur gibt es nicht zwischen den Mandanten. Die Trennung von Daten geschieht durch das von Keycloak gesteuerte Rollen und Rechtesystem. So kann kein User von einer Einrichtung auf Dokumente, Prompts oder sonstige Informationen von einer anderen Einrichtung zugreifen.
6.4	<b>Verschlüsseln</b>  Hinweis: Die unterschiedlichen Komponenten und Übertragungswege sind hierbei getrennt voneinander zu betrachten. Es muss deutlich werden, welche Verschlüsselungsverfahren zum Einsatz kommen, mit welchen Spezifika diese genutzt werden und wie das Schlüsselmanagement erfolgt. Dabei muss auch deutlich werden, welcher Personenkreis Zugriff auf die Schlüssel hat (technisch (Administratoren) und organisatorisch (fachlich Verantwortliche)).	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Siehe Ziffer 3.3 des Konzepts zur Datenspeicherung und Datenlöschung.
6.5	<b>Testen</b>  Hinweis: Das Testkonzept sollte zur Anlage genommen werden. Es muss auch dargelegt werden, mit welchen systematisch erzeugten Testdaten getestet wird.	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Siehe internes Testkonzept Dataport.

	Falls zusätzliche Tests mit personenbezogenen Daten erfolgen, sind die dafür erforderlichen Maßnahmen darzulegen	Weiter werden in der aktuellen Version der IT-Freigabeerklärung das Testvorgehen der fachlichen Leitstelle erläutert. Bei keinem Test werden personenbezogene Daten eingesetzt.
6.6	Betriebsvereinbarung  Hinweis: Ggf. existieren Vereinbarung nach dem HmbPersVG in denen die Standards einer datenschutzkonformen Verarbeitung zum Ausdruck gebracht werden.	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, aber Abschluss einer § 93er Vereinbarung (Bürokommunikation) noch dieses Jahr beabsichtigt.
6.7	Datenschutz-Erklärung  Hinweis: Falls eine Datenschutzerklärung getroffen wird, sollte diese zur Anlage genommen	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Siehe Datenschutzerklärung INTERN (für Nutzende von LLMoin) und Datenschutzerklärung EXTERN (für Bürger:innen)
6.8	Policies/Technische Maßnahme <sup>1</sup>  Hinweis: Zur Sicherheit von IT-Anwendungen, die z.B. auch von Externen ((außerhalb des FHH-Netzes) erreicht werden, tragen Policies bei, in denen konkret die Verbindungen mit implementierten IT-Sicherheitsinfrastrukturen beschrieben sind.	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Die Zugriffe auf LLMoin sind auf unterschiedliche Rollen zugeschnitten. Siehe hierzu Ziffer 4.2 „Rollenbeschreibung“ des Konzepts zur Datenspeicherung und Datenlöschung.
6.9	Datenschutzmanagement  Hinweis: Die Umsetzung des Datenschutzmanagements sollte zur Anlage genommen werden.	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Siehe Richtlinien der FHH (u.a. Beteiligungsrichtlinie, Freigaberichtlinie, Leitlinie DSB, Datenschutzrichtlinie, Entsorgungsrichtlinie)
6.10	Löschen  Hinweis: Bei der Erforderlichkeit einer DSFA ist ein „nein“ grundsätzlich nicht vorstellbar. Die Zeitpunkte der ggf. unterschiedlichen Löschungen der pers. Daten und die Umsetzung der Lösung sowie das Löschen im ergänzenden Bedarfsfall (z.B. bei unrechtmäßig erhobenen Daten im Einzelfall) sollte dargestellt werden	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  Siehe Ziffer 5.1 des Konzepts zur Datenspeicherung und Datenlöschung.
6.11	Anonymisieren	<input checked="" type="checkbox"/> ja <input type="checkbox"/> nein

<sup>1</sup> Die Policy bzw. Policies (engl. Richtlinien oder EDV-Richtlinien) bilden in der IT ein Regelwerk, das klärt, wer welche Daten sehen, lesen, bearbeiten und löschen darf. Das heißt: Mit der Einführung einer Policy können/werden auch die Rollen der Benutzer geklärt, wer welche Systeme und Services nutzen darf.



	Hinweis: Falls eine Anonymisierung erfolgt, sollte die Umsetzung der Anonymisierung dargelegt werden, um nachvollziehen zu können, ob die Anforderungen eine Anonymisierung gewährleistet werden und um ggf. die Restrisiken eine De-Anonymisierung abschätzen zu können. Hier sollte auf den Unterschied zur Pseudonymität hingewiesen werden. Falls eine Pseudonymisierung erfolgt, sollte das genutzte Verfahren dargestellt werden	Die Content Filter von Azure loggen ihre Aktivität in anonymer Form (ohne Inhaltsdaten) siehe Ziffer 5.2.9 des Konzepts zur Datenspeicherung und Datenlöschung). Geloggt wird nur, wenn die Content Filter aktiv werden.
6.12	Backup	<input type="checkbox"/> ja <input checked="" type="checkbox"/> nein  Es werden keine Backups von Datensätzen erstellt.
6.13 <sup>2</sup>	Weitere:	Klicken Sie hier, um Text einzugeben.

7. Risiken und zu gewährleistende Schutzziele		
Hinweis: Da die Risiken bezogen auf die verschiedenen zum Einsatz kommenden Mittel unterschiedlich sein können, sollte eine getrennt Betrachtung der Risiken bezogen auf die jeweiligen Mittel und dabei verarbeiteten Daten erfolgen. Zudem sollte systematisch betrachtet werden, ob das Risiko organisationsintern/-inhärent oder organisationsextern herrührt (Unterpunkte 7.X.3 Risikoquellen).		
7.1	<b>Risiko: Unrechtmäßiger Zugriff auf die Daten</b>  <b>Schutzziel: Vertraulichkeit</b>	
7.1.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Die Daten könnten im Falle eines unbefugten Zugriffs Dritter für alle denkbaren nicht bestimmungsgemäßen Zwecke verwendet werden (Scam-E-Mails, Werbung, Verkauf von Daten). Auch könnten die Daten etwa im Internet veröffentlicht werden und hierbei die Betroffenen bloßgestellt werden. Die mögliche Fremdbestimmung über die eigenen Daten verletzt das Recht auf informationelle Selbstbestimmung / Datenschutz (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG, Art. 8 GRCh) und kann bei den Betroffenen insb. zu immateriellen Schäden führen, wie finanzielle bzw. wirtschaftliche Nachteile, etwa durch Identitätsdiebstahl, betrügerische Interneteinkäufe zu ihren Lasten durch unbefugte Dritte.

<sup>2</sup> Nach den Vorgaben des BSI zum „[Risikomanagement](#)“ können weitere Risikofaktoren betrachtet werden.

7.1.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	<p>Die Daten könnten insbesondere auf den Übermittlungswegen im Rahmen von Angriffen unbefugt abgefangen werden und im Anschluss unbefugt offengelegt werden. Die Daten könnten zudem von Nutzenden unbefugt Dritten offengelegt werden.</p> <p>Mögliche Zugriffe durch Sicherheitsbehörden in den USA, die theoretisch in Form von Herausgabeanordnungen gegen den Dienstleister Microsoft denkbar sind, sind als Bedrohung nicht zu berücksichtigen, da die Prompts von Microsoft nicht gespeichert werden.</p>
7.1.3	Was sind die Risikoquellen?	<ul style="list-style-type: none"> <li>• Personen, die den beteiligten Stellen angehören (unter anderem Nutzende, Fachliche Leitstelle, Administratoren),</li> <li>• Personen, die nicht den beteiligten Stellen angehören (Bürger:innen, Hacker:innen),</li> <li>• Computerprogramme, wie z.B. Ransomware.</li> </ul>
7.1.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	<ul style="list-style-type: none"> <li>• Für Dataport gelten die folgenden Standards für Informationssicherheit und Datenschutz: ISO 27001, ISO 27018, BSI-Testat C5:2020.</li> <li>• Dataport verfügt über ein Rollen- und Berechtigungskonzept, Authentifizierungsmechanismen (siehe hierzu Konzept zur Datenspeicherung und Datenlöschung).</li> <li>• Transportverschlüsselung TLS 1.2+ für alle API-Aufrufe zwischen Client, KI-Modell und Speichersystem.</li> <li>• Speicherung und nachvollziehbare Protokollierung der Zugriffe auf Systeme.</li> <li>• Nutzungsanalysen erfolgen mit Pseudonymen anstelle von Klarnamen.</li> <li>• Ausschluss der Verarbeitung von Daten nach Art. 9 und 10 DSGVO, Daten Minderjähriger, Daten, die dem Sozial-, Berufs- und besonderen Amtsgeheimnis unterliegen, Personalaktendaten, soweit sie vertrauliche oder höchstpersönliche Daten darstellen, sowie Daten aus Personenstands- und Melderegister oder</li> </ul>

		Meldedaten mit Sperrvermerken über Handlungsanweisungen, die für LLMoin gelten und bei der Nutzung von LLMoin zu beachten sind.
7.1.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.1.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	<input checked="" type="checkbox"/> geringfügig <input type="checkbox"/> überschaubar <input type="checkbox"/> substantiell <input type="checkbox"/> groß  <p>Beschreibung:</p> <p>Bei den in LLMoin verarbeiteten Daten handelt es sich um solche, deren unbefugter Zugriff nicht zu schweren psychischen Beschwerden, finanziellen Schwierigkeiten, schweren körperlichen Beschwerden oder zu ähnlich signifikanten Konsequenzen führen würde.</p> <p>Auch die o.g. beispielhaften Folgen wie Identitätsdiebstahl und betrügerische Interneteinkäufe zu Lasten der betroffenen Person durch unbefugte Dritte sind im vorliegenden Fall unwahrscheinlich, da die hierzu erforderlichen Informationen, wie Zahlungs- und Kontodaten, in LLMoin nicht regelhaft verarbeitet werden. Bei den in LLMoin verarbeiteten Daten handelt es sich weder um besonders vertrauliche Daten noch um personenbezogene Daten besonderer Kategorien.</p>
7.1.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	<input type="checkbox"/> geringfügig <input checked="" type="checkbox"/> überschaubar <input type="checkbox"/> substantiell <input type="checkbox"/> groß  <p>Beschreibung:</p> <p>Die Eintrittswahrscheinlichkeit der Verletzung der Vertraulichkeit ist insgesamt überschaubar.</p> <p>Die Wahrscheinlichkeit unberechtigter Zugriffe durch Personen, die der Organisation angehören, ist durch eine umfassendes, dokumentiertes, granulares Rollen- und Berechtigungskonzept mit sicherer technischer Umsetzung einschließlich von Maßnahmen zur Verschlüsselung, Authentifizierung und Protokollierung erheblich reduziert.</p>

		Die Wahrscheinlichkeit unberechtigter Zugriffe durch Personal der Dataport ist durch eine sorgfältige Auswahl und Verpflichtung (Sicherheitsüberprüfung) und durch ein angemessenes Administrationskonzept erheblich reduziert.
7.2	<b>Risiko: Unerwünschte Veränderung von Daten</b>  <b>Schutzziel: Integrität</b>	
7.2.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	<ul style="list-style-type: none"> <li>• Die Informationen können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden. Hierdurch können schützenswerte Interessen der betroffenen Person an der Verarbeitung beeinträchtigt sein.</li> <li>• Bei einem Verlust der Integrität von Inhaltsdaten könnte es zu einem fehlerhaften Verwaltungsvorgang kommen, sollte der übermittelte Datensatz korruptiert und in dieser Form Grundlage der Sachbearbeitung werden.</li> <li>• Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden.</li> <li>• Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden und damit verloren gehen (Folgefehler Datenverlust).</li> <li>• Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können (Folgefehler Datenverlust).</li> </ul> <p>Ferner könnten Fehler der Integrität zur Offenbarung von Daten an Unbefugte führen (Folgefehler Bruch der Vertraulichkeit).</p>
7.2.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Die Integrität von Daten kann durch verschiedene Ursachen verletzt werden, z. B. durch Manipulationen, Fehlverhalten von Personen, Fehlbedienung von LLMoin, Fehlfunktionen von LLMoin oder Übermittlungsfehler. Konkrete Bedrohungen sind:

		<ul style="list-style-type: none"> <li>- Übertragungsfehler: Bei der Datenübertragung kann es zu Übertragungsfehlern kommen.</li> <li>- Schadprogramme: Durch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.</li> <li>- Fehleingaben: Durch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die häufig lange Zeit nicht bemerkt werden.</li> </ul> <p>Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z.B. um Zugriff auf weitere Datenbestände zu erlangen.</p>
7.2.3	Was sind die Risikoquellen?	<ul style="list-style-type: none"> <li>• Personen, die den beteiligten Stellen angehören (unter anderem Nutzende, Fachliche Leitstelle, Administratoren),</li> <li>• Personen, die nicht den beteiligten Stellen angehören (Bürger:innen, Hacker:innen),</li> <li>• Computerprogramme, wie z.B. Ransomware.</li> </ul>
7.2.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	<ul style="list-style-type: none"> <li>• Die Integrität wird unter anderem durch die nachfolgend dargestellten, ausgewählten Maßnahmen sichergestellt:</li> <li>• Zutrittssicherung zu den Gebäuden des Verantwortlichen und der Dataport.</li> <li>• Zugangssicherung mittels Authentifizierungsmechanismen (siehe hierzu Konzept zur Datenspeicherung und Datenlöschung).</li> <li>• Zugriffssicherung mittels Rollen- und Berechtigungskonzept (siehe hierzu Konzept zur Datenspeicherung und Datenlöschung).</li> <li>• Sorgfältige Auswahl und Verpflichtung des Personals bei Dataport, zusätzlich Sicherheitsüberprüfung.</li> <li>• Die im Rahmen der Nutzung von LLMoin übermittelten Daten werden mit TLS 1.2+ verschlüsselt, um unberechtigte Änderungen</li> </ul>

		<p>zu vermeiden (siehe hierzu Konzept zur Datenspeicherung und Datenlöschung).</p> <ul style="list-style-type: none"> <li>Durch die Handlungsanweisungen, die für LLMoin gelten und bei der Nutzung von LLMoin zu beachten sind, ist sichergestellt, dass die ungeprüfte Verwendung von Antworten aus LLMoin untersagt ist. Nach den Handlungsanweisungen müssen die Antworten auf sprachliche und inhaltliche Richtigkeit, Angemessenheit und Aktualität überprüft und bei Bedarf angepasst werden.</li> </ul>
7.2.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.2.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	<input checked="" type="checkbox"/> geringfügig <input type="checkbox"/> überschaubar <input type="checkbox"/> substantiell <input type="checkbox"/> groß  Beschreibung:  Der Risikoschweregrad dürfte überschaubar sein, da ausreichende Maßnahmen (siehe Ziffer 7.2.4) getroffen werden, um zu vermeiden, dass sich die aufgeworfenen Risiken realisieren.
7.2.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	<input checked="" type="checkbox"/> geringfügig <input type="checkbox"/> überschaubar <input type="checkbox"/> substantiell <input type="checkbox"/> groß  Beschreibung:  Es ist von einer geringen auszugehen, da umfassende risikoangemessene Maßnahmen (siehe Ziffer 7.2.4) getroffen werden, um zu vermeiden, dass sich die aufgeworfenen Risiken für die Integrität der Daten realisieren.
7.3	<b>Risiko: Datenverlust</b>  <b>Schutzziel: Verfügbarkeit</b>	
7.3.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Betroffene bzw. der Verantwortliche haben bei Datenverlust keinen Zugriff (mehr) auf die verarbeiteten personenbezogenen Daten. Die Geltendmachung von Betroffenenrechte läuft ins Leere, da der Verantwortliche diese nicht mehr/nur eingeschränkt erfüllen kann. Der

		<p>Verantwortliche kann seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nicht/nur eingeschränkt nachkommen.</p> <p>Der Verlust von Daten in LLMoin wird jedoch nicht zu einem Verlust der Daten insgesamt führen. In LLMoin werden in der Regel Daten verarbeitet und Dokumente hochgeladen, die außerhalb von LLMoin bereits vorhanden und damit redundant gespeichert sind.</p>
7.3.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	<p>Eine häufige Form des Datenverlustes ist, dass Daten unbeabsichtigt oder unerlaubt gelöscht werden, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware. Dies ist in Bezug auf LLMoin jedoch kein typisches Risiko.</p> <p>Ein Datenverlust kann auch durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern entstehen. Dies ist in Bezug auf LLMoin jedoch kein typisches Risiko.</p>
7.3.3	Was sind die Risikoquellen?	<ul style="list-style-type: none"> <li>• Fehlende darüberhinausgehende Speicherung der Daten und Dokumente außerhalb von LLMoin,</li> <li>• Personen, die den beteiligten Stellen angehören (unter anderem Nutzende, Fachliche Leitstelle, Administratoren),</li> <li>• Personen, die nicht den beteiligten Stellen angehören (Bürger:innen, Hacker:innen),</li> <li>• Computerprogramme, wie z.B. Ransomware</li> <li>• Naturkatastrophen</li> </ul>
7.3.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Maßnahmen sind nicht erforderlich, da die Wahrscheinlichkeit, dass Daten und Dokumente außerhalb von LLMoin nicht vorhanden sind und damit nicht redundant gespeichert sind, gering ist.
7.3.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.3.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	<p><input checked="" type="checkbox"/> geringfügig  <input type="checkbox"/> überschaubar  <input type="checkbox"/> substantiell  <input type="checkbox"/> groß</p> <p>Beschreibung:</p>

		Siehe oben Ziffer 7.3.4.
7.3.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	<input checked="" type="checkbox"/> geringfügig <input type="checkbox"/> überschaubar <input type="checkbox"/> substantiell <input type="checkbox"/> groß  Beschreibung:  Siehe oben Ziffer 7.3.4.

8. Beschreibung und Bewertung der Restrisiken:		
	Beschreibung	Bewertung des Rest-Risikos: Normal
	Die Risiken für eine Verletzung der Schutzziele haben unter Berücksichtigung der getroffenen Maßnahmen folgende Schweregrade und Eintrittswahrscheinlichkeiten: <ul style="list-style-type: none"> <li>- Vertraulichkeit               <ul style="list-style-type: none"> <li>o Schweregrad: geringfügig</li> <li>o Eintrittswahrscheinlichkeit: überschaubar</li> </ul> </li> <li>- Integrität               <ul style="list-style-type: none"> <li>o Schweregrad: geringfügig</li> <li>o Eintrittswahrscheinlichkeit: geringfügig</li> </ul> </li> <li>- Verfügbarkeit               <ul style="list-style-type: none"> <li>o Schweregrad: geringfügig</li> <li>o Eintrittswahrscheinlichkeit: geringfügig</li> </ul> </li> </ul>	Hieraus ergeben sich folgende Risikobewertungen gemäß Risikomatrix:  normal  gering  gering  Die Restrisiken sind damit insgesamt normal

9. Stellungnahme des Datenschutzbeauftragten:	
	<input checked="" type="checkbox"/> Die Verarbeitung kann so umgesetzt werden.  <input type="checkbox"/> Die Verarbeitung sollte nicht umgesetzt werden.  Begründung: Die Risiken der Datenverarbeitung in LLMoin sind durch die Handlungsanweisungen, die für LLMoin gelten und von den Nutzenden zu beachten sind, und die übrigen technischen und organisatorischen Maßnahmen hinreichend reduziert. Jedenfalls ist kein hohes Risiko für die Rechte und Freiheiten der Betroffenen erkennbar.