Large Language Models
verantwortungsvoller Einsatz in der öffentlichen Verwaltung

1. Nutzungsrechte

1.1 Der Nutzer erhält an den von Sopra Steria am Canvas „Large Language Models - verantwortungsvoller Einsatz in der öffentlichen Verwaltung“ und den im Zusammenhang damit erbrachten Arbeitsergebnissen ein einfaches (nicht ausschließliches), zeitlich und räumlich unbegrenztes Recht, die Arbeitsergebnisse für eigene interne Zwecke im Rahmen des vorausgesetzten Einsatzzwecks auf Dauer zu nutzen. Das ihm eingeräumte Nutzungsrecht an den Arbeitsergebnissen kann der Nutzer nur unter vollständiger Aufgabe der eigenen Rechte und unter der Auflage der Quellenangabe im Sinne eines Zitiergebotes an Dritte übertragen.

1.2 Die Einräumung der Nutzungsrechte erfolgt unentgeltlich mit der Übergabe an den Nutzer.

2. Haftung

2.1 Soweit nicht anderweitig zwingend gesetzlich vorgeschrieben, haftet Sopra Steria nur für die Verletzung wesentlicher Vertragspflichten (Kardinalpflichten). Kardinalpflichten sind solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung eines Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Nutzer regelmäßig vertrauen darf. Diese Haftung ist bei Sach- und Vermögensschäden auf den typischen und vorhersehbaren Schaden beschränkt.

2.2 Die Haftung ist im Falle von leichter Fahrlässigkeit aufgrund der Unentgeltlichkeit der Nutzung ausgeschlossen.

2.3 Die Haftung für eventuellen Datenverlust oder -beschädigung ist auf den Aufwand beschränkt, der bei ordnungsgemäßer Datensicherung erforderlich wäre, um die Daten aus dem gesicherten Datenmaterial wiederherzustellen.

2.4 Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von eventuell eingebundenen gesetzlichen Vertretern und Erfüllungsgehilfen von Sopra Steria.

2.5 Die Verwendung von Begriffen wie Garantie, Zusicherung, Sicherstellen oder zugesicherte Eigenschaft begründet aus sich selbst keine Garantie i.S.d. BGB, sondern ist ausschließlich leistungsbeschreibend zu verstehen. Sofern Garantieerklärungen abgegeben werden sollen, bedürfen sie einer gesonderten, schriftlichen Vereinbarung.

2.6 Haftungsansprüche verjähren nach einem Jahr. Dies gilt nicht, soweit das Gesetz bei einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung von Sopra Steria sowie in den Fällen der Verletzung des Lebens, des Körpers oder der Gesundheit eine längere Frist vorschreibt.

3. Vertraulichkeit & Datenschutz

3.1 Der Nutzer und Sopra Steria werden sämtliche ihnen im Rahmen des Austauschs mündlich, schriftlich oder in sonstiger Weise direkt oder indirekt bekanntwerdende, als vertraulich bezeichneten oder der Natur der Sache nach üblicherweise als vertraulich anzusehenden Informationen oder Informationsmaterialien – auch solche, die nicht unter das Geschäftsgeheimnisgesetz fallen – vertraulich behandeln und diese ausschließlich im Rahmen der von diesen Nutzungsbedingungen erfassten Leistungen verwenden.

3.2 Ausgenommen von dieser Geheimhaltungspflicht sind nur solche Informationen und Informationsmaterialien, die

a. zur Zeit ihres Bekanntwerdens bereits offenkundig, d.h. jedem Dritten ohne weiteres zugänglich sind,

b. dem Nutzer oder Sopra Steria nach Bekanntwerden rechtmäßig von einem Dritten zugänglich gemacht werden, der diesbezüglich keiner Geheimhaltungspflicht gegenüber dem anderen unterliegt,

c. auf Verlangen einer Behörde oder eines sonst berechtigten Dritten dieser bzw. diesem zwingend mitzuteilen sind,

d. Rechts- oder Steuerberatern des jeweiligen anderen zum Zwecke der Beratung notwendigerweise mitgeteilt werden müssen.

In den Fällen der Unterpunkte c) und d) werden sich Nutzer und Sopra Steria – soweit rechtlich zulässig – unverzüglich über ein entsprechendes Verlangen und vor der Weitergabe von geschützten Informationen informieren.

3.3 Der Nutzer und Sopra Steria werden sämtlichen Mitarbeitern oder Dritten, die sie im Kontext einsetzen, schriftlich eine entsprechende Geheimhaltungsverpflichtung auferlegen.

3.4 Die Vertraulichkeit wirkt auf unbestimmte Zeit fort.

3.5 Dem Nutzer und Sopra Steria ist bekannt, dass eine elektronische und unverschlüsselte Kommunikation (z.B. per E-Mail, per Download) mit Sicherheitsrisiken verbunden ist. Bei dieser Art der Kommunikation werden sie daher keine Ansprüche geltend machen, die durch das Fehlen einer Verschlüsselung begründet sind, soweit nicht anderweitig eine Verschlüsselung vereinbart ist.

4. Schlussbestimmungen

4.1 Abweichende Vertrags- / Bestellbedingungen des Nutzers finden keine Anwendung. Dies gilt auch dann, wenn Sopra Steria diesen Bedingungen nicht ausdrücklich widerspricht.

4.2 Änderungen und Ergänzungen dieser Bedingungen bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

4.3 Gerichtsstand ist Hamburg. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).

4.4 Sollte eine Bestimmung dieser Nutzungsbedingungen nichtig oder anfechtbar oder aus einem sonstigen Grunde unwirksam sein oder werden, so bleiben diese im Übrigen wirksam. Der Nutzer und Sopra Steria verpflichten sich, in einem solchen Fall statt der nichtigen, anfechtbaren oder unwirksamen Bestimmung eine solche zu vereinbaren, die ihrem angestrebten Zweck möglichst nahekommt und einen entsprechenden wirtschaftlichen Erfolg gewährleistet. § 139 BGB findet keine Anwendung.

Large Language Models
verantwortungsvoller Einsatz in der öffentlichen Verwaltung

Stammdaten

Name
… des Use Cases

Team
… Teilnehmer:innen des Teams

Problem Space

Beispiel
Beispielhafte Ausführung des Use Cases…

Detaillierte Beschreibung
z.B. Benutzererfahrung, Wachstum, Höhere Geschwindigkeit, reduzierte Komplexität/Risiko, Effizienzsteigerung, ...

Solution Space

Gewünschtes Ergebnis der Lösung

Vorteile
z.B. Benutzererfahrung, Wachstum, Höhere Geschwindigkeit, reduzierte Komplexität/Risiko, Effizienzsteigerung, ...

LLM-Input

LLM-Output
Wie könnte die Ausgabe des LLM aussehen? Bis zu welchem Grad wären Fehler akzeptabel? Wie wird der Output weiter verarbeitet bzw. genutzt?

LLM-Funktion

- ☐ **Extrahierung & Filterung**, z.B. Informationen finden oder Schlüsselwörter extrahieren
- ☐ **Anonymisierung & Maskierung**, z.B. Namen im Text ersetzen
- ☐ **Verbesserung & Erweiterung**, z.B. Text ausschmücken oder ergänzen
- ☐ **Erkennung & Vorhersage**, z.B. die nächste Aktion oder Konsequenz vorhersagen
- ☐ **Zusammenfassung & Erklärung**, z.B. Text kürzen oder Humor erklären
- ☐ **Umwandlung & Übersetzung**, z.B. Code in eine andere Programmiersprache übersetzen oder einen Text vereinfachen
- ☐ **Sonstiges: .....**

Risk Space

Primär betroffene Prinzipien
Die drei wichtigsten Prinzipien für den Usecase sind…

- ☐ Transparenz und Verantwortlichkeit
- ☐ Gleichheit und Unparteilichkeit
- ☐ Datenschutz und -Sicherheit
- ☐ Bürgerbeteiligung und Vertrauen
- ☐ Verlässlichkeit und Planbarkeit
- ☐ Handeln im Sinne des Gemeinwohls
- ☐ Effizienz
- ☐ Qualität des Outputs

Relevante Herausforderungen
Die wichtigsten Herausforderungen bei dem Usecase sind…

- ☐ Trainingsdaten-Bias
- ☐ Verstärkung bestehender Machtdynamiken
- ☐ Confirmation Bias
- ☐ Halluzinationen
- ☐ Überprüfbarkeit
- ☐ Fehlende Anwendungsfallspezifische Benchmarks
- ☐ Rechtssicherheit (Nachvollziehbarkeit + Verantwortung)
- ☐ Souveränität über Eingabedaten
- ☐ privater Einfluss (Interessenskonflikte mit Anbietern)
- ☐ Vertrauensverlust in der Bevölkerung
- ☐ Inkonsistenzen

Passende Maßnahmen

- ☐ Eigenes Modell entwickeln
- ☐ Kontextanpassung durch Fine-Tuning
- ☐ eXplainable AI
- ☐ Angemessene Datenbereinigung, -Assessment, -Auswahl, -Anonymisierung
- ☐ Parameteroptimierung
- ☐ automatische Validierung / Tests
- ☐ (Training in) Prompt Engineering
- ☐ Genaue Vorgaben für den Einsatz in der öffentl. Verwaltung
- ☐ Protokollierung / (externe) Audits
- ☐ Meldung von Qualitätsproblemen und Korrektur von Ergebnissen
- ☐ Diverse Teams
- ☐ Vier-Augen-Entscheidungen
- ☐ Output-Prüfung durch Expert*Innen
- ☐ …

aric

sopra steria