European Commission

Procurement of AI Community

PUBLIC BUYERS COMMUNITY

Vorschlag für Standardvertragsklauseln für die Beschaffung von Systemen der künstlichen Intelligenz durch öffentliche Einrichtungen

Version vom September 2023 (draft) – High Risk version

Haftungsausschluss

Dieses Dokument ist ein Entwurf und dient ausschließlich als Diskussionsgrundlage, um erste Rückmeldungen von Interessenträgern einzuholen. Der Autor dieses Dokuments ist Jeroen Naves (Pels Rijcken). Dies ist kein offizielles EU-Dokument und es darf unter keinen Umständen als Dokument gesehen werden, das den offiziellen Standpunkt der Europäischen Kommission wiedergibt. Weder die Europäische Kommission noch in ihrem Namen handelnde Personen können für die Verwendung der in diesem Dokument enthaltenen Informationen verantwortlich gemacht werden. Die Ausarbeitung dieses Dokuments ist noch nicht abgeschlossen.

Vorbemerkungen

Diese Standardvertragsklauseln wurden für öffentliche Einrichtungen verfasst, die ein von einem externen Lieferanten entwickeltes KI-System beschaffen möchten. Diese Standardklauseln basieren auf den Standardklauseln für die Beschaffung von algorithmischen Systemen, die von der Stadt Amsterdam im Jahr 2018 ausgearbeitet wurden (https://www.amsterdam.nl/innovatie/digitalisering-technologie/algoritmen-ai/contractual-terms-for-algorithms/).

Die in diesem Entwurf enthaltenen Standardvertragsklauseln stützen sich weitgehend auf die Anforderungen und Verpflichtungen in Bezug auf Hochrisiko-KI-Systeme gemäß Titel III des Vorschlags für eine Verordnung über künstliche Intelligenz* (im Folgenden „KI-Gesetz“). Dieser Vorschlag ist derzeit noch Gegenstand von Verhandlungen; das bedeutet, die Klauseln müssen noch überarbeitet werden, um etwaigen Änderungen Rechnung zu tragen und sie vollständig an die vom Rat und vom Europäischen Parlament angenommene endgültige Verordnung anzupassen.

Da die Verhandlungen über das vorgeschlagene KI-Gesetz noch nicht abgeschlossen sind, können öffentliche Einrichtungen, die sich für die Anwendung dieser Bedingungen entscheiden, dies auf freiwilliger Basis tun und im Einzelfall prüfen, ob die verschiedenen Abschnitte dieser Standardvertragsklauseln für die Beschaffung eines bestimmten KI-Systems ausreichend und angemessen sind. Die Standardvertragsklauseln erstrecken sich insbesondere auf KI-Systeme, die als „Hochrisiko-Systeme“ im Sinne des Artikels 6 eingestuft werden und unter einen der in den Anhängen II und III des vorgeschlagenen KI-Gesetzes aufgeführten Bereiche fallen. Für KI-Systeme, die kein hohes Risiko darstellen, ist die Anwendung dieser Anforderungen im Rahmen des KI-Gesetzes zwar nicht zwingend vorgeschrieben, wird aber empfohlen, um die Vertrauenswürdigkeit der von öffentlichen Einrichtungen beschafften KI-Anwendungen zu erhöhen. Sofern es angemessen und angesichts der Auswirkungen des Systems auf den Einzelnen und die Gesellschaft gerechtfertigt ist, können öffentliche Einrichtungen diese Klauseln auch auf andere, nicht zwangsläufig als „KI-Systeme“ eingestufte algorithmische Systeme anwenden, um auch einfachere regelbasierte Software-Systeme zu erfassen, da bei deren Einsatz im öffentlichen Sektor in bestimmten Fällen ebenfalls eine erhöhte Rechenschaftspflicht, Kontrolle und Transparenz geboten sein kann.

Für öffentliche Einrichtungen, die diese Standardvertragsklauseln auf KI-Systeme, die kein hohes Risiko darstellen, anwenden möchten, ist auch eine vereinfachte Version der Klauseln verfügbar.

Die Standardvertragsklauseln enthalten nur Bestimmungen, die sich konkret auf KI-Systeme und auf Angelegenheiten im Geltungsbereich des vorgeschlagenen KI-Gesetzes beziehen; das heißt, sie umfassen keine sonstigen Verpflichtungen oder Anforderungen, die sich aus einschlägigen geltenden Rechtsvorschriften wie etwa der Datenschutz-Grundverordnung ergeben können. Ferner stellen diese Standardvertragsklauseln keine vollständige vertragliche Vereinbarung dar. Beispielsweise enthalten diese Standardvertragsklauseln keine Auflagen in Bezug auf geistiges Eigentum, Abnahme, Zahlung, Lieferfristen, anwendbares Recht oder Haftung. Die Standardvertragsklauseln sind so formuliert, dass sie einem Vertrag, in dem diese Punkte bereits geregelt sind, als Anhang beigefügt werden können.

* Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union (COM(2021) 206 final).

Abschnitt A – Begriffsbestimmungen

Article 1 Begriffsbestimmungen

1.1. Für die Zwecke dieser Klauseln gelten folgende Begriffsbestimmungen:

- Vertrag: der gesamte Vertrag, dessen integraler Bestandteil die als Anhang beigefügten Klauseln sind;
- KI-System: das/die in **Anhang A** genannte(n) KI-System(e), einschließlich neuer Versionen davon;
- Klauseln: die vorliegenden Standardvertragsklauseln für die Beschaffung von Systemen der künstlichen Intelligenz durch öffentliche Einrichtungen;
- Datensätze der öffentlichen Einrichtung: Datensätze (oder Teile davon), i) die die öffentliche Einrichtung dem Lieferanten im Rahmen des Vertrags zur Verfügung stellt oder ii) die im Rahmen des Vertrags erstellt oder erfasst werden, einschließlich der (z. B. durch Kommentierung, Kennzeichnung, Bereinigung, Anreicherung und Aggregierung) geänderten oder erweiterten Versionen der unter i) und ii) genannten Datensätze;
- Datensätze: alle bei der Entwicklung des KI-Systems verwendeten Datensätze, einschließlich des oder der in **Anhang B** beschriebenen Datensatzes oder Datensätze;
- Lieferung: der Zeitpunkt, zu dem der Lieferant der öffentlichen Einrichtung mitteilt, dass das KI-System alle vereinbarten Bedingungen erfüllt und einsatzbereit ist;
- Zweckbestimmung: die Verwendung, für die ein KI-System laut der öffentlichen Einrichtung bestimmt ist, einschließlich der in Anhang B aufgeführten besonderen Nutzungsumstände und Nutzungsbedingungen entsprechend den Angaben des Lieferanten in der Gebrauchsanweisung, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation;
- vernünftigerweise vorhersehbare Fehlanwendung: die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen ergeben kann;
- wesentliche Änderung: eine nach der Lieferung vorgenommene Änderung des KI-Systems, die sich auf die Konformität des KI-Systems mit den in diesen Klauseln enthaltenen Anforderungen auswirkt oder zu einer Änderung der Zweckbestimmung führt;
- Lieferant: eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die der öffentlichen Einrichtung das KI-System gemäß dem Vertrag liefert;
- Datensätze des Lieferanten und Datensätze von Dritten: Datensätze (oder Teile davon), die nicht als Datensätze öffentlicher Organisationen gelten.

Abschnitt B – Grundlegende Anforderungen an das KI-System

Article 2 Risikomanagementsystem

2.1. Der Lieferant stellt sicher, dass vor der Lieferung des KI-Systems ein Risikomanagementsystem für das KI-System eingerichtet und angewandt wird.

2.2. Das Risikomanagementsystem umfasst zumindest die folgenden Schritte:

a. Ermittlung, Abschätzung und Bewertung der bekannten und vernünftigerweise vorhersehbaren Risiken für die Gesundheit, die Sicherheit und die in der Europäischen Union geltenden Grundrechte, die unter Berücksichtigung der Zweckbestimmung des KI-Systems und einer vernünftigerweise vorhersehbaren Fehlanwendung auftreten können;
b. Bewertung anderer möglicherweise auftretender Risiken;
c. Ergreifung angemessener und gezielter Risikomanagementmaßnahmen zur Bewältigung der gemäß den Buchstaben a und b dieses Absatzes ermittelten Risiken im Einklang mit den Bestimmungen der folgenden Absätze.

2.3. Die in Artikel 2 Absatz 2 Buchstabe c genannten Risikomanagementmaßnahmen werden so gestaltet, dass die mit einer bestimmten Gefahr verbundenen einschlägigen Restrisiken sowie das Gesamtrestrisiko des KI-Systems vom Lieferanten nach vernünftigem Ermessen als vertretbar beurteilt werden können, sofern das KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird.

2.4. Bei der Festlegung der am besten geeigneten Risikomanagementmaßnahmen nach Artikel 2 Absatz 2 Buchstabe c ist Folgendes sicherzustellen:
a. Beseitigung oder Verringerung der ermittelten Risiken, soweit dies technisch möglich ist, durch eine geeignete Konzeption und Entwicklung des KI-Systems;
b. gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen im Hinblick auf nicht auszuschließende Risiken;
c. Bereitstellung angemessener Informationen durch die öffentliche Einrichtung.

2.5. Der Lieferant stellt sicher, dass das KI-System vor seiner Lieferung getestet wird, um zu überprüfen, ob das KI-System den Klauseln entspricht und ob die in Artikel 2 Absatz 2 Buchstabe c genannten Risikomanagementmaßnahmen unter Berücksichtigung der Zweckbestimmung und einer vernünftigerweise vorhersehbaren Fehlanwendung wirksam sind. Auf Verlangen der öffentlichen Einrichtung ist der Lieferant verpflichtet, das KI-System in der Umgebung der öffentlichen Einrichtung zu testen.

2.6. Alle im Zusammenhang mit der Einhaltung der Bestimmungen dieses Artikels erkannten Risiken, getroffenen Maßnahmen und durchgeführten Tests müssen vom Lieferanten dokumentiert werden. Der Lieferant muss der öffentlichen Einrichtung die entsprechenden Unterlagen spätestens zum Zeitpunkt der Lieferung des KI-Systems zur Verfügung stellen. Die Unterlagen können auch im Rahmen der technischen Dokumentation und/oder der Gebrauchsanweisung bereitgestellt werden.

2.7. Das Risikomanagementsystem versteht sich als ein kontinuierlicher und iterativer Prozess während der gesamten Laufzeit des Vertrags. Nach der Lieferung des KI-Systems ist der Lieferant somit verpflichtet:
a. das Risikomanagementverfahren regelmäßig zu überprüfen und zu aktualisieren, um dessen fortdauernde Wirksamkeit sicherzustellen;
b. die Dokumentation gemäß Artikel 2 Absatz 6 auf dem neuesten Stand zu halten und
c. jede neue Version der Dokumentation gemäß Artikel 2 Absatz 6 der öffentlichen Einrichtung unverzüglich zur Verfügung zu stellen.

2.8. Wenn es für die ordnungsgemäße Anwendung des Risikomanagementsystems durch den Lieferanten nach vernünftigem Ermessen erforderlich ist, stellt die öffentliche Einrichtung

dem Lieferanten auf Anfrage Informationen zur Verfügung, sofern diese nicht vertraulich sind.

2.9. **<Fakultativ>** Nutzt die öffentliche Einrichtung das KI-System über die Laufzeit des Vertrags hinaus, stellt der Lieferant der öffentlichen Einrichtung am Ende der Laufzeit des Vertrags die Informationen zur Verfügung, die die öffentliche Einrichtung benötigt, um das Risikomanagementsystem selbst weiter zu betreiben.

Article 3 **< Artikel 3 ist nur für KI-Systeme relevant, in denen Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden. Artikel 3 setzt voraus, dass der Lieferant (oder seine Unterauftragnehmer) vollen Zugang zu den Datensätzen hat (bzw. haben). Wenn sich die Datensätze ausschließlich im Besitz der öffentlichen Einrichtung befinden, sind andere Vereinbarungen zu treffen.>** Daten und Daten-Governance

3.1. Der Lieferant stellt sicher, dass die bei der Entwicklung des KI-Systems verwendeten Datensätze, einschließlich der Trainings-, Validierungs- und Testdatensätze, einer dem Kontext der Nutzung und der Zweckbestimmung des KI-Systems angemessenen Data-Governance unterworfen wurden bzw. werden. Die damit verbundenen Maßnahmen betreffen insbesondere:

a. die Transparenz in Bezug auf den ursprünglichen Zweck der Datenerfassung;
b. die einschlägigen konzeptionellen Entscheidungen;
c. die Verfahren zur Datenerfassung;
d. Datenaufbereitungsvorgänge wie Kommentierung, Kennzeichnung, Bereinigung, Anreicherung und Aggregierung;
e. die Aufstellung relevanter Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen;
f. eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), bei denen davon auszugehen ist, dass sie die Gesundheit und Sicherheit natürlicher Personen beeinträchtigen oder zu einer nach dem Recht der Europäischen Union verbotenen Diskriminierung führen;
g. geeignete Maßnahmen zur Erkennung, Verhinderung und Minderung möglicher Verzerrungen;
h. die Ermittlung einschlägiger Datenlücken oder Mängel, die die Einhaltung dieser Klauseln verhindern, und wie diese Lücken und Mängel behoben werden können.

3.2. Der Lieferant stellt sicher, dass die bei der Entwicklung des KI-Systems verwendeten Datensätze im Hinblick auf die Zweckbestimmung relevant, repräsentativ, so weit wie möglich fehlerfrei und möglichst vollständig sind. Der Lieferant stellt sicher, dass die Datensätze die geeigneten statistischen Merkmale haben, gegebenenfalls auch bezüglich der Personen oder Personengruppen, auf die das KI-System bestimmungsgemäß angewandt werden soll. Diese Merkmale der Datensätze werden durch einzelne Datensätze oder eine Kombination solcher Datensätze erfüllt.

3.3. Der Lieferant stellt sicher, dass die bei der Entwicklung des KI-Systems verwendeten Datensätze, soweit dies unter Berücksichtigung der Zweckbestimmung oder einer vernünftigerweise vorhersehbaren Fehlanwendung erforderlich ist, den Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder

funktionalen Rahmenbedingungen des jeweiligen Kontexts, in dem das KI-System bestimmungsgemäß verwendet werden soll, typisch sind.

3.4. Die Verpflichtungen aus diesem Artikel gelten nicht nur für die Entwicklung des KI-Systems vor der Lieferung, sondern auch für jede Verwendung von Datensätzen durch den Lieferanten, die das Funktionieren des KI-Systems zu irgendeinem anderen Zeitpunkt während der Vertragslaufzeit beeinträchtigen kann.

Article 4 Technische Dokumentation und Gebrauchsanweisung

4.1. Die Lieferung des KI-Systems durch den Lieferanten umfasst die Aushändigung der technischen Dokumentation und der Gebrauchsanweisung.

4.2. Anhand der technischen Dokumentation muss es der öffentlichen Einrichtung oder einem Dritten möglich sein, die Konformität des KI-Systems mit den in diesen Klauseln festgelegten Anforderungen zu bewerten, und die technische Dokumentation muss mindestens die in **Anhang C** beschriebenen Voraussetzungen erfüllen.

4.3. Die Gebrauchsanweisung enthält präzise, vollständige, korrekte und eindeutige Informationen in einer für die öffentliche Einrichtung relevanten, barrierefrei zugänglichen und verständlichen Form. Die Gebrauchsanweisung muss mindestens die in **Anhang D** beschriebenen Voraussetzungen erfüllen.

4.4. Der Lieferant muss diese Dokumentation zumindest bei jeder wesentlichen Änderung während der Laufzeit des Vertrags aktualisieren und sie anschließend der öffentlichen Einrichtung zur Verfügung stellen.

4.5. **<Fakultativ>** Die technische Dokumentation und die Gebrauchsanweisung müssen in englischer Sprache abgefasst sein.

4.6. **<Fakultativ>** Die öffentliche Einrichtung hat unbeschadet der Bestimmungen der Artikel 6 und 13 das Recht, Kopien der technischen Dokumentation und der Gebrauchsanweisung anzufertigen, soweit dies für die interne Verwendung innerhalb der öffentlichen Einrichtung erforderlich ist.

Article 5 Aufzeichnungspflichten

5.1. Der Lieferant stellt sicher, dass das KI-System mit Funktionsmerkmalen konzipiert und entwickelt wurde bzw. wird, die eine automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung") während des Betriebs des KI-Systems ermöglichen. Diese Protokollierung muss dem Stand der Technik und, sofern vorhanden, anerkannten Normen oder gemeinsamen Spezifikationen entsprechen. **<Fakultativ: spezifische Norm einfügen, sofern vorhanden>**

5.2. Die Protokollierung gewährleistet, dass das Funktionieren des KI-Systems während seines gesamten Lebenszyklus in einem Maße rückverfolgbar ist, das der Zweckbestimmung des Systems und der vernünftigerweise vorhersehbaren Fehlanwendung angemessen ist. Insbesondere muss die Protokollierung die Aufzeichnung von Ereignissen ermöglichen, die für die Ermittlung von Situationen relevant sind, die:

a. dazu führen können, dass das KI-System ein Risiko für die Gesundheit oder Sicherheit oder den Schutz der Grundrechte von Personen darstellt, oder

b. zu einer wesentlichen Änderung führen.

5.3. **<Fakultativ>** Der Lieferant ermöglicht es der öffentlichen Einrichtung, in Echtzeit auf die vom KI-System automatisch erzeugten Protokolle zuzugreifen.

5.4. Der Lieferant bewahrt die vom KI-System automatisch erzeugten Protokolle für die Laufzeit des Vertrags auf, soweit diese Protokolle gemäß dem Vertrag seiner Kontrolle unterliegen. Am Ende der Laufzeit des Vertrags stellt der Lieferant diese Protokolle unverzüglich der öffentlichen Einrichtung zur Verfügung.

Article 6 Transparenz des KI-Systems

6.1. Der Lieferant stellt sicher, dass das KI-System so konzipiert und entwickelt wurde bzw. wird, dass der Betrieb des KI-Systems hinreichend transparent ist, damit die öffentliche Einrichtung die Funktionsweise des Systems in angemessener Weise nachvollziehen kann.

6.2. Um für eine angemessene Transparenz zu sorgen, muss der Lieferant vor der Lieferung des KI-Systems zumindest die in **Anhang E** beschriebenen technischen und organisatorischen Maßnahmen umsetzen. Durch diese Maßnahmen sollte die öffentliche Einrichtung in der Lage sein, das KI-System angemessen zu verstehen und zu nutzen. Hierfür sollte die öffentliche Einrichtung ein verstehen, wie das KI-System funktioniert und welche Daten von ihm verarbeitet werden, damit sie den Personen oder Personengruppen, auf die das KI-System angewandt wird bzw. werden soll, die vom KI-System getroffenen Entscheidungen erklären kann.

Article 7 Menschliche Aufsicht

7.1. Der Lieferant stellt sicher, dass das KI-System so konzipiert und entwickelt wurde bzw. wird, dass es je nach den von ihm ausgehenden Risiken – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden kann.

7.2. Der Lieferant stellt sicher, dass vor der Lieferung geeignete Maßnahmen in das KI-System integriert und umgesetzt werden, um die menschliche Aufsicht zu gewährleisten. Diese Maßnahmen, zu denen unter anderem eine Schulung der Beschäftigten der öffentlichen Einrichtung zählen kann, müssen den Personen, denen die menschliche Aufsicht übertragen wurde, je nach den Umständen Folgendes ermöglichen:

a. die relevanten Fähigkeiten und Grenzen des KI-Systems zu kennen und vollständig zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, damit Anzeichen von Anomalien, Fehlfunktionen und unerwarteter Leistung so bald wie möglich erkannt und behoben werden können;

b. sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in das von einem KI-System hervorgebrachte Ergebnis („Automatisierungsbias“) bewusst zu bleiben, insbesondere wenn das KI-System Informationen oder Empfehlungen ausgibt, auf deren Grundlage natürliche Personen Entscheidungen treffen;

c. die Ergebnisse des KI-Systems richtig zu interpretieren, wobei insbesondere die Merkmale des Systems und die vorhandenen Interpretationswerkzeuge und -methoden zu berücksichtigen sind;

d. in einer bestimmten Situation zu beschließen, das KI-System nicht zu verwenden oder das Ergebnis des KI-Systems anderweitig außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen;

e. in den Betrieb des KI-Systems einzugreifen oder den Systembetrieb mit einer „Stopptaste" oder einem ähnlichen Verfahren zu unterbrechen.

7.3. **<Fakultativ>** Um für eine angemessene menschliche Aufsicht zu sorgen, muss der Lieferant vor der Lieferung des KI-Systems zumindest die in **Anhang F** beschriebenen technischen und organisatorischen Maßnahmen umsetzen.

Article 8 Genauigkeit, Robustheit und Cybersicherheit

8.1. Der Lieferant stellt sicher, dass das KI-System nach den Grundsätzen der konzeptionsintegrierten Sicherheit („Security by Design") und der Sicherheit durch Voreinstellungen („Security by Default") konzipiert und entwickelt wurde bzw. wird. Im Hinblick auf seine Zweckbestimmung sollte das KI-System ein angemessenes Maß an Genauigkeit, Robustheit, allgemeiner Sicherheit und Cybersicherheit erreichen und in dieser Hinsicht während seines gesamten Lebenszyklus beständig funktionieren.

8.2. Die Genauigkeitsgrade und die relevanten Genauigkeitskennzahlen des KI-Systems sind in **Anhang G** beschrieben.

8.3. Um für ein angemessenes Maß an Robustheit, allgemeiner Sicherheit und Cybersicherheit zu sorgen, muss der Lieferant vor der Lieferung des KI-Systems zumindest die in **Anhang H** beschriebenen technischen und organisatorischen Maßnahmen umsetzen.

Abschnitt C – Pflichten des Lieferanten in Bezug auf das KI-System

Article 9 Erfüllung der Anforderungen von Abschnitt B

Der Lieferant muss sicherstellen, dass das KI-System vom Zeitpunkt seiner Lieferung bis zum Ende der Laufzeit des Vertrags die in Abschnitt B dieser Klauseln festgelegten Anforderungen erfüllt.

Article 10 **<Fakultativ>** Qualitätsmanagementsystem

10.1. Vor der Lieferung des AI-Systems richtet der Lieferant ein Qualitätsmanagementsystem ein, das die Einhaltung dieser Klauseln gewährleistet. Dieses System wird systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert und umfasst mindestens folgende Aspekte:

a. ein Konzept zur Einhaltung der Regulierungsvorschriften;

b. Techniken, Verfahren und systematische Maßnahmen für den Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des KI-Systems;

c. Techniken, Verfahren und systematische Maßnahmen für die Entwicklung, Qualitätskontrolle und Qualitätssicherung des KI-Systems;

d. Untersuchungs-, Test- und Validierungsverfahren, die vor, während und nach der Entwicklung des KI-Systems durchzuführen sind, und die Häufigkeit der Durchführung;

e. die technischen Spezifikationen und Normen, die anzuwenden sind, und – falls die einschlägigen harmonisierten Normen nicht vollständig angewandt werden oder nicht alle einschlägigen Anforderungen abdecken – die Mittel, mit denen gewährleistet werden soll, dass das KI-System die Anforderungen in Abschnitt B dieser Klauseln erfüllt;

f. Systeme und Verfahren für das Datenmanagement, einschließlich Datenerfassung, Datenanalyse, Datenkennzeichnung, Datenspeicherung, Datenfilterung, Datenauswertung, Datenaggregation, Vorratsdatenspeicherung und sonstiger Vorgänge in Bezug auf die Daten, die im Vorfeld der Lieferung des KI-Systems durchgeführt werden;

g. das in Artikel 2 genannte Risikomanagementsystem;

h. Verfahren zur Meldung schwerwiegender Vorfälle und Fehlfunktionen;

i. Systeme und Verfahren für die Aufzeichnung aller einschlägigen Unterlagen und Informationen;

j. Ressourcenmanagement, einschließlich Maßnahmen im Hinblick auf die Versorgungssicherheit;

k. einen Rechenschaftsrahmen, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf alle in diesem Absatz aufgeführten Aspekte regelt.

Article 11 **<Fakultativ>** Konformitätsbewertung

11.1. Der Lieferant stellt sicher, dass das KI-System vor seiner Lieferung dem folgenden Konformitätsbewertungsverfahren unterzogen wird:

a. Der Lieferant überprüft, ob das bestehende Qualitätsmanagementsystem den Anforderungen des Artikels 10 entspricht.

b. Der Lieferant prüft die in der technischen Dokumentation enthaltenen Informationen, um zu beurteilen, ob das KI-System den einschlägigen grundlegenden Anforderungen in Abschnitt B dieser Klauseln entspricht.

c. Der Lieferant überprüft ferner, ob der Entwurfs- und Entwicklungsprozess des KI-Systems mit der technischen Dokumentation im Einklang steht.

11.2. Der Lieferant stellt sicher, dass das KI-System einem neuen Konformitätsbewertungsverfahren unterzogen wird, wenn er während der Laufzeit des Vertrags wesentliche Änderungen daran vornimmt.

Article 12 Korrekturmaßnahmen

Wenn der Lieferant während der Vertragslaufzeit – entweder aufgrund einer Bemerkung der öffentlichen Einrichtung oder aus einem anderen Grund – der Auffassung ist oder Grund zu der Annahme hat, dass das KI-System nicht diesen Klauseln entspricht, ergreift er unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität des Systems herzustellen. Der Lieferant setzt die öffentliche Einrichtung davon in Kenntnis.

Article 13 Pflicht zur Erläuterung der Funktionsweise des KI-Systems auf individueller Ebene

13.1. Zusätzlich zu den in Artikel 6 beschriebenen Verpflichtungen ist der Lieferant während der Laufzeit des Vertrags verpflichtet, die öffentliche Einrichtung auf deren erstes Ersuchen dabei zu unterstützen, zu erläutern, wie das KI-System zu einer bestimmten Entscheidung oder einem bestimmten Ergebnis gegenüber den Personen oder Personengruppen, auf die das KI-System angewandt wird bzw. werden soll, gelangt ist. Diese Unterstützung umfasst zumindest eindeutige Angaben dazu, anhand welcher Schlüsselfaktoren das KI-System ein bestimmtes Ergebnis hervorgebracht hat, und wie die Eingaben geändert werden müssen, damit das System ein anderes Ergebnis hervorbringt.

13.2. Im Rahmen der in Artikel 13 Absatz 1 beschriebenen Verpflichtung sind der öffentlichen Einrichtung alle technischen und sonstigen Informationen zur Verfügung zu stellen, die erforderlich sind, um zu erklären, wie das KI-System zu einer bestimmten Entscheidung oder einem bestimmten Ergebnis gelangt ist, und um den Personen oder Personengruppen, auf die das KI-System angewandt wird bzw. werden soll, die Möglichkeit zu geben, die Art und Weise, wie das KI-System zu einer bestimmten Entscheidung oder einem bestimmten Ergebnis gelangt ist, zu überprüfen. Der Lieferant räumt der öffentlichen Einrichtung hierfür das Recht ein, diese Informationen zu verwenden, weiterzugeben und offenzulegen, wenn und soweit dies erforderlich ist, um die Personen oder Personengruppen, auf die das KI-System angewandt wird bzw. werden soll, über die Funktionsweise des KI-Systems zu informieren, und/oder wenn und soweit dies in etwaigen Gerichtsverfahren erforderlich ist.

13.3. **<Fakultativ>** Im Rahmen der in Artikel 13 Absätze 1 und 2 aufgeführten Pflichten ist Folgendes bereitzustellen: der Quellcode des KI-Systems, die bei der Entwicklung des KI-Systems verwendeten technischen Spezifikationen, die Datensätze, technische Informationen darüber, wie die bei der Entwicklung des KI-Systems verwendeten Datensätze gewonnen und bearbeitet wurden, Informationen über die verwendete Entwicklungsmethode und den durchgeführten Entwicklungsprozess, die Begründung der Wahl eines bestimmten Modells und seiner Parameter sowie Informationen über die Leistung des KI-Systems.

Abschnitt D – Rechte zur Nutzung der Datensätze

Article 14 Rechte an Datensätzen der öffentlichen Einrichtung

14.1. Alle Rechte im Zusammenhang mit Datensätzen der öffentlichen Einrichtung, einschließlich aller Rechte des geistigen Eigentums, stehen der öffentlichen Einrichtung oder einem von der öffentlichen Einrichtung benannten Dritten zu.

14.2. Der Lieferant ist nicht berechtigt, Datensätze der öffentlichen Einrichtung für andere Zwecke als die Erfüllung des Vertrags zu nutzen, sofern in Anhang B nichts anderes bestimmt ist.

14.3. Auf erstes Ersuchen der öffentlichen Einrichtung muss der Lieferant die Datensätze der öffentliche Einrichtung vernichten, sofern in Anhang B nichts anderes bestimmt ist. Wenn die öffentliche Einrichtung dies verlangt, muss der Lieferant einen geeigneten Nachweis über die Vernichtung der Datensätze der öffentlichen Einrichtung vorlegen.

Article 15 Rechte an Datensätzen des Lieferanten und Datensätzen von Dritten

15.1. Alle Rechte im Zusammenhang mit Datensätzen des Lieferanten oder Datensätzen von Dritten, einschließlich aller Rechte des geistigen Eigentums, stehen dem Lieferanten bzw. den Dritten zu.

15.2. Sofern in Anhang B nichts anderes bestimmt ist, gewährt der Lieferant der öffentlichen Einrichtung ein nicht ausschließliches Recht zur Nutzung der Datensätze des Lieferanten und der Datensätze von Dritten, das in jedem Fall ausreicht, um die Bestimmungen des Vertrags, einschließlich der Klauseln, zu erfüllen.

15.3. **<Fakultativ>** Das in Artikel 15 Absatz 2 beschriebene Nutzungsrecht schließt das Recht für die öffentliche Einrichtung oder einen Dritten ein, die Datensätze des Lieferanten und die Datensätze von Dritten für die Weiterentwicklung des KI-Systems, einschließlich neuer Versionen davon, zu nutzen.

Article 16 Aushändigung der Datensätze

16.1. Auf erstes Ersuchen der öffentlichen Einrichtung händigt der Lieferant der öffentlichen Einrichtung die aktuellste Version der Datensätze der öffentlichen Einrichtung aus.

16.2. Auf erstes Ersuchen der öffentlichen Einrichtung händigt der Lieferant der öffentlichen Einrichtung die aktuellste Version der Datensätze des Lieferanten und der Datensätze von Dritten aus, sofern in Anhang B nichts anderes bestimmt ist.

16.3. Der Lieferant muss der öffentlichen Einrichtung die Datensätze in einem gängigen, von der öffentlichen Einrichtung zu bestimmenden Dateiformat bereitstellen. **<Fakultativ> Die Datensätze werden folgendermaßen zurückgegeben: [Dateiformat].**

Article 17 Freistellung von Ansprüchen

17.1. Der Lieferant stellt die öffentliche Einrichtung im Hinblick auf die Datensätze des Lieferanten und die Datensätze von Dritten von allen Ansprüchen, die von Dritten, einschließlich von Aufsichtsbehörden, aufgrund der Verletzung ihrer Rechte des geistigen Eigentums oder Datenschutzrechte erhoben werden, oder von entsprechenden Ansprüchen, die in Bezug auf Wissen, unzulässigen Wettbewerb usw. erhoben werden, frei.

17.2. Die öffentliche Einrichtung stellt den Lieferanten im Hinblick auf die Datensätze der öffentlichen Einrichtung von allen Ansprüchen, die von Dritten, einschließlich von Aufsichtsbehörden, aufgrund der Verletzung ihrer Rechte des geistigen Eigentums oder Datenschutzrechte erhoben werden, oder von entsprechenden Ansprüchen, die in Bezug auf Wissen, unzulässigen Wettbewerb usw. erhoben werden, frei.

Abschnitt E – KI-Register und Audit

Article 18 **<Fakultativ>** KI-Register

18.1. Auf erstes Ersuchen der öffentlichen Einrichtung stellt der Lieferant der öffentlichen Einrichtung die aktuellste Version der in Anhang C und Anhang D aufgeführten Informationen zur Verfügung.

18.2. Die öffentliche Einrichtung ist berechtigt, die in Artikel 18 Absatz 1 dargelegten Informationen an Dritte weiterzugeben und beispielsweise in einem Register für KI-Systeme zu veröffentlichen.

18.3. Auf Verlangen der öffentlichen Einrichtung ist der Lieferant bei der Eintragung der KI-Systeme in ein entsprechendes Register behilflich.

Article 19 Einhaltung der Bestimmungen und Audit

19.1. Auf erstes Ersuchen der öffentlichen Einrichtung muss der Lieferant der öffentlichen Einrichtung alle Informationen zur Verfügung stellen, die für den Nachweis der Einhaltung dieser Klauseln erforderlich sind.

19.2. Der Lieferant ist verpflichtet, bei einem Audit oder einer anderen Art von Inspektion mitzuwirken, die von der öffentlichen Einrichtung oder in deren Namen durchgeführt wird, um festzustellen, ob der Lieferant seinen in diesen Klauseln festgelegten Verpflichtungen jederzeit nachkommt. Die Mitwirkung durch den Lieferanten umfasst die Bereitstellung aller von der öffentlichen Einrichtung geforderten Informationen, die Gewährung von Einblicken in das implementierte Risikomanagementsystem, die Bereitstellung von Personal für Befragungen und die Gewährung des Zugangs zu den Standorten des Lieferanten.

19.3. Die öffentliche Einrichtung erstellt einen Bericht oder veranlasst die Erstellung eines Berichts, in dem die Ergebnisse des Audits festgehalten werden. In dem Bericht hält die öffentliche Einrichtung fest, inwieweit der Lieferant den Pflichten aus dem Vertrag nachkommt. Stellt die öffentliche Einrichtung fest, dass der Lieferant den Pflichten gemäß diesem Artikel nicht nachkommt, ist der Lieferant verpflichtet, die von der öffentlichen Einrichtung festgestellten Mängel innerhalb einer von der öffentlichen Einrichtung in dem Bericht festgelegten angemessenen Frist zu beheben. Versäumt es der Lieferant, die von der öffentlichen Einrichtung festgestellten Mängel innerhalb der im Bericht für die Mängelbehebung festgelegten Frist zu beheben, so gerät er von Rechts wegen in Verzug.

19.4. Die öffentliche Einrichtung ist berechtigt, die Ergebnisse des in Artikel 19 Absatz 3 genannten Berichts zu veröffentlichen.

19.5. Die öffentliche Einrichtung ist berechtigt, einmal pro Kalenderjahr oder im Zusammenhang mit einer wesentlichen Änderung ein Audit durchzuführen oder durchführen zu lassen.

19.6. Die öffentliche Einrichtung kann beschließen, das Audit ganz oder teilweise von einem unabhängigen Prüfer durchführen zu lassen.

19.7. Sollten durch die Beauftragung eines Prüfers Kosten entstehen, so werden diese von der öffentlichen Einrichtung getragen. Die öffentliche Einrichtung zahlt dem Lieferanten eine angemessene Gebühr zur Deckung der Kosten, die diesem im Zusammenhang mit dem Audit entstehen. Im Falle von Streitigkeiten über die Höhe dieser Gebühr ist der Lieferant unter keinen Umständen berechtigt, seine Pflichten im Rahmen dieser Klauseln auszusetzen. Die öffentliche Einrichtung muss keine Gebühr zahlen, wenn das Audit ergibt, dass der Lieferant seinen Pflichten im Rahmen dieser Klauseln nicht nachgekommen ist.

Abschnitt F – Kosten

Article 20 Kosten

Sofern die Parteien nichts anderes vereinbart haben oder in diesen Klauseln nicht ausdrücklich etwas anderes vorgesehen ist, muss die öffentliche Einrichtung dem Lieferanten für die Arbeiten, die sich aus diesen Klauseln ergeben, keine weiteren Gebühren zahlen.

Anhang A – Das KI-System und die Zweckbestimmung

Beschreibung des KI-Systems

In den Geltungsbereich dieser Klauseln fallen die folgenden Systeme oder Systemkomponenten:

Bitte beschreiben Sie das/die KI-System(e). Dabei kann es sich auch um ein algorithmisches System handeln, das nicht als KI-System im Sinne des KI-Gesetzes gilt.

Zweckbestimmung

Bitte beschreiben Sie den Verwendungszweck des KI-Systems.

Anhang B – Die Datensätze

Bitte beschreiben Sie die Datensätze, die für das Training (sofern zutreffend), die Validierung und das Testen der KI-Systeme verwendet werden. Unterscheiden Sie dabei zwischen Datensätzen der öffentlichen Einrichtung und Datensätzen des Lieferanten sowie Datensätzen von Dritten. Im Falle von Datensätzen der öffentlichen Einrichtung beschreiben Sie, für welche Zwecke (abgesehen von der Ausführung des Vertrags) der Lieferant die Datensätze verwenden darf, und geben Sie an, ob der Lieferant verpflichtet ist, die Datensätze am Ende der Vertragslaufzeit zu vernichten. Im Falle von Datensätzen des Lieferanten und Datensätzen von Dritten beschreiben Sie, für welche Zwecke die öffentliche Einrichtung die Datensätze verwenden darf, und geben Sie an, ob der Lieferant verpflichtet ist, die Datensätze auszuhändigen.

Datensätze der öffentlichen Einrichtung

Die folgenden Datensätze werden dem Lieferanten von der öffentlichen Einrichtung im Rahmen des Vertrags zur Verfügung gestellt oder sind im Rahmen des Vertrags zu erstellen bzw. zu erfassen:

Beschreibung des Datensatzes	**Nutzungsrechte des Lieferanten**	**Verpflichtung zur Vernichtung des Datensatzes am Ende der Vertragslaufzeit**
		Ja/Nein
		Ja/Nein
		Ja/Nein
		Ja/Nein

Datensätze des Lieferanten und Datensätze von Dritten

Die folgenden Datensätze des Lieferanten und Datensätze von Dritten werden oder wurden für das Training (sofern zutreffend), die Validierung und das Testen des KI-Systems verwendet:

Beschreibung des Datensatzes	**Nutzungsrechte der öffentlichen Einrichtung**	**Verpflichtung zur Aushändigung[1]**
		Ja/Nein
		Ja/Nein

[1] Eine Einschränkung der Verpflichtung zur Aushändigung von Datensätzen des Lieferanten und Datensätzen von Dritten führt nicht zu einer Einschränkung der in den Artikeln 6 und 13 beschriebenen Pflichten des Lieferanten.

		Ja/Nein
		Ja/Nein

Anhang C – Technische Dokumentation

Die technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende KI-System von Belang sind:

1. allgemeine Beschreibung des KI-Systems, einschließlich folgender Angaben:
   - 1.1. Zweckbestimmung, Name des Lieferanten, Datum und Version des Systems;
   - 1.2. Art der Daten, die durch das System voraussichtlich verarbeitet werden oder bestimmungsgemäß verarbeitet werden sollen, und – im Falle personenbezogener Daten – die Kategorien von natürlichen Personen und Gruppen, die voraussichtlich oder bestimmungsgemäß betroffen sein werden;
   - 1.3. gegebenenfalls Art und Weise, wie das KI-System mit Hardware oder Software, die nicht Teil des KI-Systems selbst sind, interagieren kann oder verwendet werden kann;
   - 1.4. Versionen der betreffenden Software oder Firmware und etwaige Anforderungen in Bezug auf die Aktualisierung der Versionen;
   - 1.5. Beschreibung aller Formen, in denen das KI-System in Verkehr gebracht oder in Betrieb genommen wird;
   - 1.6. Beschreibung der Hardware, auf der das KI-System betrieben werden soll;
   - 1.7. falls das KI-System Bestandteil von Produkten ist: Fotografien oder Abbildungen, die äußere Merkmale, Kennzeichnungen und den inneren Aufbau dieser Produkte zeigen;
   - 1.8. detaillierte und leicht verständliche Beschreibung des wichtigsten Optimierungsziels bzw. der wichtigsten Optimierungsziele des Systems;
   - 1.9. detaillierte und leicht verständliche Beschreibung der zu erwartenden Ergebnisse des Systems und der zu erwartenden Qualität dieser Ergebnisse;
   - 1.10. detaillierte und leicht verständliche Anweisungen zur Interpretation der Ergebnisse des Systems;
   - 1.11. Beispiele für Szenarien, für die das System nicht verwendet werden sollte;

2. detaillierte Beschreibung der Bestandteile des KI-Systems und seines Entwicklungsprozesses, einschließlich folgender Angaben:
   - 2.1. Methoden und Schritte zur Entwicklung des KI-Systems, gegebenenfalls einschließlich des Einsatzes von Dritten bereitgestellter vortrainierter Systeme oder Werkzeuge, und wie diese vom Lieferanten benutzt, integriert oder verändert wurden, einschließlich einer Beschreibung aller Lizenz- oder sonstigen vertraglichen Vereinbarungen im Zusammenhang mit solchen Beiträgen Dritter;
   - 2.2. Entwurfsspezifikationen des Systems, insbesondere die allgemeine Logik des KI-Systems und der Algorithmen; wichtigste Entwurfsentscheidungen mit den Gründen und Annahmen, auch in Bezug auf Personen oder Personengruppen, auf die das System angewandt werden soll; hauptsächliche Klassifizierungsentscheidungen; was das System optimieren soll und welche Bedeutung den verschiedenen Parametern dabei zukommt; Entscheidungen über mögliche Kompromisse in Bezug auf die technischen Lösungen, mit denen die Anforderungen nach diesen Klauseln erfüllt werden sollen;

2.3. Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen oder einander zuarbeiten und in die Gesamtverarbeitung integriert sind; zum Entwickeln, Trainieren, Testen und Validieren des KI-Systems verwendete Rechenressourcen;

2.4. gegebenenfalls Datenanforderungen in Form von Datenblättern, in denen die Trainingsmethoden und -techniken und die verwendeten Trainingsdatensätze beschrieben werden, mit Angaben zu Herkunft, Umfang und Hauptmerkmalen dieser Datensätze; Angaben zur Beschaffung und Auswahl der Daten; Kennzeichnungsverfahren (z. B. für überwachtes Lernen), Datenbereinigungsmethoden (z. B. Erkennung von Ausreißern);

2.5. gegebenenfalls detaillierte Beschreibung der vorab bestimmten Änderungen an dem KI-System und seiner Leistung mit allen einschlägigen Angaben zu den technischen Lösungen, mit denen sichergestellt wird, dass das KI-System die einschlägigen Anforderungen nach diesen Klauseln weiterhin dauerhaft erfüllt;

2.6. verwendete Validierungs- und Testverfahren, mit Angaben zu den verwendeten Validierungs- und Testdaten und deren Hauptmerkmalen; Parameter, die zur Messung der Genauigkeit, Robustheit, Cybersicherheit und der Erfüllung anderer einschlägiger Anforderungen nach diesen Klauseln sowie potenziell diskriminierender Auswirkungen verwendet werden; Testprotokolle und alle von den verantwortlichen Personen datierten und unterzeichneten Testberichte, auch in Bezug auf die in Nummer 2.5 genannten vorab bestimmten Änderungen;

2.7. Angaben zu ergriffenen Cybersicherheitsmaßnahmen;

detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems, insbesondere in Bezug auf: seine Fähigkeiten und Leistungsgrenzen, mit dem Genauigkeitsgrad für bestimmte Personen oder Personengruppen, auf die das System angewandt werden soll, und dem insgesamt erwarteten Genauigkeitsgrad in Bezug auf seine Zweckbestimmung; vorhersehbare unbeabsichtigte Ergebnisse und Risikoquellen für die Gesundheit und Sicherheit, die Grundrechte und eine etwaige Diskriminierung angesichts der Zweckbestimmung des KI-Systems;

3. detaillierte Beschreibung des Risikomanagementsystems gemäß Artikel 2;

4. Beschreibung aller relevanten Änderungen, die der Lieferant während des Lebenszyklus des Systems an dem System vorgenommen hat.

Anhang D – Gebrauchsanweisung

Die Gebrauchsanweisung muss mindestens die folgenden Informationen enthalten, soweit sie für das KI-System von Belang sind:

1. den Namen und die Kontaktangaben des Lieferanten sowie gegebenenfalls seines Bevollmächtigten;

2. die Merkmale, Fähigkeiten und Leistungsgrenzen des KI-Systems, gegebenenfalls einschließlich folgender Angaben:
   - 2.1. Zweckbestimmung;
   - 2.2. Maß an Genauigkeit, Robustheit und Cybersicherheit gemäß Artikel 8, für das das KI-System getestet und validiert wurde und das zu erwarten ist, sowie alle eindeutig bekannten und vorhersehbaren Umstände, die sich auf das erwartete Maß an Genauigkeit, Robustheit und Cybersicherheit auswirken können;
   - 2.3. alle eindeutig bekannten oder vorhersehbaren Umstände im Zusammenhang mit der Zweckbestimmung des KI-Systems oder einer vernünftigerweise vorhersehbaren Fehlanwendung, die zu Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können;
   - 2.4. Angaben dazu, inwieweit das KI-System eine Erklärung für seine Entscheidungen liefern kann;
   - 2.5. seine Leistung bezüglich der Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll;
   - 2.6. relevante Informationen über Eingriffe der Nutzer, die die Systemleistung beeinflussen können, einschließlich Angaben über die Art oder Qualität der Eingabedaten oder sonstiger relevanter Informationen über die verwendeten Trainings-, Validierungs- und Testdatensätze unter Berücksichtigung der Zweckbestimmung des KI-Systems;

3. etwaige Änderungen des KI-Systems und seiner Leistung, die der Lieferant vorab bestimmt hat;

4. die in Artikel 7 genannten Maßnahmen zur Gewährleistung der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um der öffentlichen Einrichtung die Interpretation der Ergebnisse des KI-Systems zu erleichtern;

5. die erwartete Lebensdauer des KI-Systems und alle erforderlichen Wartungs- und Pflegemaßnahmen zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates;

6. eine Beschreibung der im KI-System enthaltenen Mechanismen, anhand derer die Nutzer die Protokolle ordnungsgemäß erfassen, speichern und auswerten können.

Anhang E – Maßnahmen zur Gewährleistung der Transparenz

Bitte beschreiben Sie hier die technischen und organisatorischen Maßnahmen, die der Lieferant zu ergreifen hat, um die Transparenz gemäß Artikel 6 der Klauseln zu gewährleisten.

Anhang F – Maßnahmen zur Gewährleistung der menschlichen Aufsicht

Bitte beschreiben Sie hier die technischen und organisatorischen Maßnahmen, die der Lieferant zu ergreifen hat, um die menschliche Aufsicht gemäß Artikel 7 der Klauseln zu gewährleisten.

Anhang G – Genauigkeitsgrade

Bitte beschreiben Sie hier die erforderlichen Genauigkeitsgrade.

Anhang H – Maßnahmen zur Gewährleistung eines angemessenen Maßes an Robustheit, allgemeiner Sicherheit und Cybersicherheit

Bitte beschreiben Sie hier die technischen und organisatorischen Maßnahmen, die der Lieferant zu ergreifen hat, um ein angemessenes Maß an Robustheit, allgemeiner Sicherheit und Cybersicherheit gemäß Artikel 8 der Klauseln zu gewährleisten.

Durch diese Maßnahmen muss sichergestellt werden, dass das KI-System möglichst widerstandsfähig gegenüber Fehlern, Störungen oder Unstimmigkeiten ist, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, insbesondere wegen seiner Interaktion mit natürlichen Personen oder anderen Systemen auftreten können.

Das KI-System muss widerstandsfähig gegenüber Versuches unbefugter Dritter sein, seine Verwendung, sein Verhalten, seine Ergebnisse oder seine Leistung durch Ausnutzung von Systemschwachstellen zu verändern. Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen zur Verhinderung, Erkennung, Erwiderung, Bewältigung und Kontrolle von Angriffen, mit denen versucht wird, den Trainingsdatensatz oder für das Training verwendete vortrainierte Komponenten zu manipulieren („Datenvergiftung“ bzw. „Modellvergiftung“), von Eingaben, die das Modell zu Fehlern verleiten sollen („feindliche Beispiele“ oder „Modellumgehung“), von Angriffen auf die Vertraulichkeit oder von Modellmängeln, die zu schädlichen Entscheidungen führen könnten.