

## KI-Mustervertragsklauseln

Die Parteien haben sich – ungeachtet der Frage, ob die jeweiligen KI-Systeme als Hochrisiko-Systeme im Sinne von Art.6 KI-VO (Verordnung (EU) 2024/1689), einzustufen sind – in dieser Anlage auf „KI-Mustervertragsklauseln“ geeinigt. Diese basieren auf einem besonders strengen Maßstab in Form der Standardvertragsklauseln für die Beschaffung von Systemen der künstlichen Intelligenz durch öffentliche Einrichtungen in der High-Risk-Varianten (MVK-KI-Hochrisiko). Sie gelten unabhängig von der Einstufung des vertragsgegenständlichen KI-Systems als Hochrisiko-KI-System nach Art. 6 KI-VO, sofern die jeweiligen Bestimmungen nicht ausdrücklich eine Anwendung ausschließlich für Hochrisiko-Systeme vorsehen und damit insoweit eine partielle Abweichung von dem strengen Maßstab zulassen.

Diese Anlage sowie die zugehörigen Anhänge sind jeweils bezogen auf einen bestimmten Einzelauftrag/Vertrag zu lesen und auszufüllen.

### Abschnitt A – Begriffsbestimmungen

Artikel 1 Begriffsbestimmungen: Für die Zwecke dieser Anlage gelten folgende Begriffsbestimmungen:

Rahmenvereinbarung: der EVB-IT-Vertragstext, dem diese KI-Mustervertragsklauseln als Anlage beigelegt sind

Vertrag: der jeweilige Einzelauftrag nach der Rahmenvereinbarung, dessen integraler Bestandteil diese KI-Mustervertragsklauseln in der auf diesen Einzelauftrag bezogenen Ausgestaltung werden;

Öffentliche Einrichtung: der jeweilige Bezugsberechtigte, dem das KI-System gemäß dem Vertrag geliefert/ bereitgestellt wird;

KI-System: das/die maschinengestützte(n) System(e), das/die für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das/die nach seiner Betriebsaufnahme anpassungsfähig sein kann/können und das/die aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet/ableiten, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können, wie in **Anhang A** näher dargelegt und beschrieben, einschließlich aller neuen Versionen davon;<sup>1</sup>

~~MVK-KI-Hochrisiko: die vorliegenden Klauseln für die Vergabe öffentlicher Aufträge für Hochrisiko-KI 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

---

<sup>1</sup> [The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application | Gestaltung der digitalen Zukunft Europas.](#)

## Anlage Nr. 06 – KI-Mustervertragsklauseln

Aggregation) 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, einschließlich anderen KI-Systemen, ergeben kann;

Wesentliche Änderung: eine nach der Lieferung vorgenommene Änderung des KI-Systems, die in der vom Lieferanten durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit **dieser Anlage** (unbeschadet von Kapitel III Abschnitt 2 der KI-Verordnung) beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde;

Lieferant: **der Auftragnehmer**, der der öffentlichen Einrichtung das KI-System gemäß dem Vertrag liefert/ **bereitstellt**;

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**

### Artikel 2 Risikomanagementsystem

- 2.1. Der Lieferant stellt sicher, dass vor der Lieferung des KI-Systems ein Risikomanagementsystem für das KI-System eingerichtet, angewandt, dokumentiert und aufrechterhalten wird.
- 2.2. Das Risikomanagementsystem umfasst zumindest die folgenden Schritte:
  - a. die Ermittlung, Abschätzung und Bewertung der bekannten und vernünftigerweise vorhersehbaren Risiken, die vom KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird,
  - b. die Abschätzung und Bewertung der Risiken, die entstehen können, wenn das KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird,
  - c. die Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem System zur Beobachtung nach dem Inverkehrbringen,
  - d. die Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen zur Bewältigung der gemäß Buchstabe a dieses Absatzes ermittelten Risiken im Einklang mit den Bestimmungen der folgenden Absätze.
- 2.3. Die in diesem Artikel genannten Risiken betreffen nur solche Risiken, die durch die Entwicklung oder Konzeption des KI-Systems oder durch die Bereitstellung ausreichender technischer Informationen angemessen gemindert oder behoben werden können.
- 2.4. Bei den in diesem Artikel genannten Risiken werden die Auswirkungen und möglichen Wechselwirkungen, die sich aus der kombinierten Anwendung der Anforderungen des Abschnitts B ergeben, gebührend berücksichtigt, um die Risiken wirksamer zu minimieren und gleichzeitig ein angemessenes Gleichgewicht bei der Durchführung der Maßnahmen zur Erfüllung dieser Anforderungen sicherzustellen.
- 2.5. Die in Artikel 2 Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden so gestaltet, dass jedes mit einer bestimmten Gefahr verbundene relevante Restrisiko sowie das Gesamtrisiko des KI-Systems vom Lieferanten nach vernünftigem Ermessen als vertretbar beurteilt werden, sofern das KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird.
- 2.6. Bei der Festlegung der am besten geeigneten Risikomanagementmaßnahmen nach Artikel 2 Absatz 2 Buchstabe d ist Folgendes sicherzustellen:
  - a. soweit technisch möglich, Beseitigung oder Verringerung der gemäß Artikel 2 Absatz 2 ermittelten und bewerteten Risiken durch eine geeignete Konzeption und Entwicklung des KI-Systems,
  - b. gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen zur Bewältigung nicht auszuschließender Risiken;
  - c. Bereitstellung angemessener Informationen für die öffentliche Einrichtung und gegebenenfalls entsprechende Schulung der Betreiber.

## Anlage Nr. 06 – KI-Mustervertragsklauseln

- 2.7. Der Lieferant stellt sicher, dass das KI-System vor seiner Lieferung getestet wird, um zu überprüfen, ob es **dieser Anlage** entspricht und ob die in Artikel 2 Absatz 2 Buchstabe d 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.
- 2.8. Das Testen des KI-Systems erfolgt zu jedem geeigneten Zeitpunkt während des gesamten Entwicklungsprozesses und in jedem Fall vor der Lieferung. Das Testen erfolgt anhand vorab festgelegter Metriken und Wahrscheinlichkeitsschwellenwerte, die für die Zweckbestimmung des KI-Systems geeignet sind.
- 2.9. 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.
- 2.10. Das Risikomanagementsystem versteht sich als ein kontinuierlicher und iterativer Prozess, der während der gesamten Laufzeit des Vertrags geplant und durchgeführt wird. Nach der Lieferung des KI-Systems ist der Lieferant **für die Laufzeit des Vertrags** somit verpflichtet:
- a. das Risikomanagementverfahren regelmäßig zu überprüfen und zu aktualisieren, um dessen fortdauernde Wirksamkeit sicherzustellen,
  - b. die Dokumentation gemäß Artikel 2 Absatz 7 auf dem neuesten Stand zu halten und
  - c. jede neue Version der Dokumentation gemäß Artikel 2 Absatz 7 der öffentlichen Einrichtung unverzüglich zur Verfügung zu stellen.
- 2.11. 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.
- 2.12. **<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.

### Artikel 3 Daten und Daten-Governance

- 3.1. Der Lieferant stellt sicher, dass **etwaige im gesamten Entwicklungsprozess** des KI-Systems **vom Lieferanten** verwendeten Datensätze, einschließlich der Trainings-, Validierungs- und Testdatensätze, Daten-Governance- und Datenmanagementverfahren unterworfen wurden bzw. werden, die der Zweckbestimmung des KI-Systems angemessen sind. Die damit verbundenen Maßnahmen betreffen insbesondere:
- a. die einschlägigen konzeptionellen Entscheidungen,
  - b. die Datenerhebungsverfahren und die Herkunft der Daten und im Falle personenbezogener Daten den ursprünglichen Zweck der Datenerhebung,

## Anlage Nr. 06 – KI-Mustervertragsklauseln

- c. relevante Datenaufbereitungsvorgänge wie Annotation, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregation,
  - d. die Aufstellung von Annahmen in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,
  - e. eine Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze,
  - f. eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der Union verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen,
  - g. geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher gemäß Buchstabe f ermittelter Verzerrungen,
  - h. die Ermittlung einschlägiger Datenlücken oder Mängel, die die Einhaltung dieser **Anlage** verhindern, und wie diese Lücken und Mängel behoben werden können.
- 3.2. Der Lieferant stellt sicher, dass **etwaige im gesamten Entwicklungsprozess** des KI-Systems **vom Lieferanten** verwendeten Datensätze im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sind. Der Lieferant stellt sicher, dass die Datensätze die geeigneten statistischen Merkmale haben, gegebenenfalls auch bezüglich der Personen oder Personengruppen, für die das KI-System bestimmungsgemäß verwendet werden soll. Diese Merkmale der Datensätze werden durch einzelne Datensätze oder eine Kombination solcher Datensätze erfüllt.
- 3.3. Der Lieferant stellt sicher, dass **etwaige im gesamten Entwicklungsprozess** des KI-Systems **vom Lieferanten** verwendeten Datensätzen, soweit dies unter Berücksichtigung der Zweckbestimmung oder einer vernünftigerweise vorhersehbaren Fehlanwendung erforderlich ist, die Merkmale oder Elemente berücksichtigt wurden, 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 auch für jede Verwendung von Datensätzen durch den Lieferanten **nach Inbetriebnahme oder Inverkehrbringen des KI-Systems während der Vertragslaufzeit**, die das Funktionieren des KI-Systems beeinträchtigen kann.

## Artikel 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 **dieser Anlage** festgelegten Anforderungen zu bewerten, und die technische Dokumentation muss mindestens die in **Anhang C** beschriebenen Voraussetzungen erfüllen.

## Anlage Nr. 06 – KI-Mustervertragsklauseln

- 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 deutscher Sprache abgefasst sein.
- 4.6. ~~<Fakultativ>~~ Die öffentliche Einrichtung hat unbeschadet der Bestimmungen der Artikel 6 und 14 das Recht, Kopien der technischen Dokumentation und der Gebrauchsanweisung anzufertigen, soweit dies für die interne Verwendung innerhalb der öffentlichen Einrichtung erforderlich ist.

### Artikel 5 Aufzeichnungspflichten

- 5.1. Der Lieferant stellt sicher, dass die Technik des KI-Systems die automatische Aufzeichnung von Ereignissen (im Folgenden „Protokollierung“) während des Lebenszyklus des Systems ermöglicht.
- 5.2. Die Protokollierung gewährleistet, dass das KI-System 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.

### Artikel 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 Ausgaben des Systems angemessen interpretieren und verwenden 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.

Artikel 7 Menschliche Aufsicht

- 7.1. Der Lieferant stellt sicher, dass das KI-System so konzipiert und entwickelt wurde bzw. wird, dass es während der Zeit seiner Nutzung – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden kann.
- 7.2. Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte, die entstehen können, wenn ein KI-System im Einklang mit seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird, wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Abschnitts fortbestehen.
- 7.3. Die Aufsichtsmaßnahmen müssen den Risiken, dem Grad der Autonomie und dem Kontext der Nutzung des KI-Systems angemessen sein und werden durch eine oder beide der folgenden Arten von Vorkehrungen gewährleistet:
- 7.4. Der Lieferant stellt sicher, dass vor der Lieferung geeignete Maßnahmen in das KI-System integriert und umgesetzt werden, um die menschliche Aufsicht zu gewährleisten. Mit diesen Maßnahmen wird sichergestellt, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, angemessen und verhältnismäßig in der Lage sind:
  - a. die einschlägigen Fähigkeiten und Grenzen des KI-Systems angemessen zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, einschließlich in Bezug auf das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung,
  - b. sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in die Ausgaben eines KI-Systems („Automatisierungsbias“) bewusst zu bleiben, insbesondere wenn das KI-System Informationen oder Empfehlungen ausgibt, auf deren Grundlage natürliche Personen Entscheidungen treffen,
  - c. die Ausgaben des KI-Systems richtig zu interpretieren, wobei unter anderem 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 die Ausgabe 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, was dem System ermöglicht, in einem sicheren Zustand zum Stillstand zu kommen.
- 7.5. **<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, **sofern ein solcher Anhang im Vertrag vereinbart wurde.**

Artikel 8 Genauigkeit, Robustheit und Cybersicherheit



- 8.1. Der Lieferant stellt sicher, dass das KI-System so konzipiert und entwickelt wurde bzw. wird, dass es ein angemessenes Maß an Genauigkeit, Robustheit, allgemeiner Sicherheit und Cybersicherheit erreicht und in dieser Hinsicht beständig funktioniert.
- 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.
- 8.4. Diese Anforderung gilt unbeschadet der Anforderungen, die sich aus Artikel 15 der KI-Verordnung ergeben.

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

### Artikel 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 **Anlage** festgelegten Anforderungen erfüllt.

### Artikel 10 Qualitätsmanagementsystem (nur bei einem Hochrisiko-System nach Art. 6 KI-VO)

- 10.1. Vor der Lieferung des KI-Systems richtet der Lieferant ein Qualitätsmanagementsystem ein, das die Einhaltung dieser **Anlage** gewährleistet.
- 10.2. Das Qualitätsmanagementsystem 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 **Anlage** erfüllt,
  - f. Systeme und Verfahren für das Datenmanagement, einschließlich Datenerfassung, Datengewinnung, 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,
  - i. die Handhabung der Kommunikation mit zuständigen nationalen Behörden, anderen einschlägigen Behörden, auch Behörden, die den Zugang zu Daten gewähren oder erleichtern, notifizierten Stellen, anderen Akteuren, Kunden oder sonstigen interessierten Kreisen,
  - j. Systeme und Verfahren für die Aufzeichnung aller einschlägigen Unterlagen und Informationen,
  - k. Ressourcenmanagement, einschließlich Maßnahmen im Hinblick auf die Versorgungssicherheit,
  - l. einen Rechenschaftsrahmen, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf alle in diesem Absatz aufgeführten Aspekte regelt.
- 10.3. Während der Laufzeit des Vertrags muss der Lieferant die das Qualitätsmanagementsystem betreffenden Unterlagen bereithalten. Auf erstes Ersuchen der öffentlichen Einrichtung händigt der Lieferant der öffentlichen Einrichtung die aktuellste Version der das Qualitätsmanagementsystem betreffenden Unterlagen aus.

Artikel 11 Konformitätsbewertung (nur bei einem Hochrisiko-System nach Art. 6 KI-VO)

- 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 Anlage 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.

Artikel 12 <Fakultativ> Folgenabschätzung in Bezug auf die Grundrechte

<Fakultativ> Auf erstes Ersuchen der öffentlichen Einrichtung wirkt der Lieferant an der von der öffentlichen Einrichtung durchgeführten Bewertung der Auswirkungen mit, die die Nutzung des KI-Systems auf die Grundrechte haben könnte.

Artikel 13 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 dieser **Anlage** entspricht, ergreift er unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität des Systems herzustellen. Der Lieferant setzt die öffentliche Einrichtung davon in Kenntnis.

### Artikel 14      **<Fakultativ>** Pflicht zur Erläuterung der Entscheidungsfindung im Einzelfall

- 14.1. **<Fakultativ>** Neben den in Artikel 6 beschriebenen Verpflichtungen ist der Lieferant verpflichtet, die öffentliche Einrichtung auf deren erstes Ersuchen dabei zu unterstützen, die Rolle des KI-Systems im Entscheidungsverfahren klar und verständlich zu erläutern, **sofern das KI-System zu einer Entscheidungsfindung, von der natürliche Personen betroffen sind, eingesetzt wird.** Diese verständliche Erläuterung sollte Personen, die von einer von der öffentlichen Einrichtung auf der Grundlage der Ausgaben des KI-Systems getroffenen Entscheidung betroffen sind, insbesondere (aber nicht ausschließlich) Einblicke in die wichtigsten Elemente der Entscheidung vermitteln.
- 14.2. **<Fakultativ>** Im Rahmen der in Artikel 14 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 eine bestimmte Ausgabe hervorgebracht hat, und um den betroffenen Personen die Möglichkeit zu geben, die Art und Weise, wie das KI-System eine bestimmte Ausgabe hervorgebracht hat, zu überprüfen. Der Lieferant räumt der öffentlichen Einrichtung hiermit das Recht ein, diese Informationen zu nutzen, weiterzugeben und offenzulegen, sofern und soweit dies erforderlich ist, um die betroffenen Personen entsprechend zu informieren.
- 14.3. **<Fakultativ>** ~~Im Rahmen der in Artikel 14 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

### Artikel 15      Rechte an Datensätzen der öffentlichen Einrichtung

- 15.1. 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.

- 15.2. 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.
- 15.3. Auf erstes Ersuchen der öffentlichen Einrichtung muss der Lieferant die Datensätze der öffentlichen 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.

Artikel 16      Rechte an Datensätzen des Lieferanten und Datensätzen von Dritten

- 16.1. 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.
- 16.2. 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 **dieser Anlage**, zu erfüllen.
- 16.3. **<Fakultativ>** Das in Artikel 16 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.

Artikel 17      Aushändigung der Datensätze

- 17.1. Auf erstes Ersuchen der öffentlichen Einrichtung händigt der Lieferant der öffentlichen Einrichtung die aktuellste Version der Datensätze der öffentlichen Einrichtung aus.
- 17.2. 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.
- 17.3. Der Lieferant muss der öffentlichen Einrichtung die Datensätze in einem gängigen, von der öffentlichen Einrichtung zu bestimmenden Dateiformat bereitstellen. Die Datensätze werden, **wie im Vertrag vereinbart**, zurückgegeben.

Artikel 18      Freistellung von Ansprüchen

- 18.1. Der Lieferant stellt die öffentliche Einrichtung von allen Ansprüchen frei, die von Dritten, einschließlich Aufsichtsbehörden, geltend gemacht werden, wenn die Nutzung des KI-Systems, der Datensätze des Lieferanten und/oder der Datensätze von Dritten durch die öffentliche Einrichtung dazu geführt hat, dass Rechte des geistigen Eigentums, Datenschutzrechte oder gleichwertige Rechte verletzt wurden.
- 18.2. Die öffentliche Einrichtung stellt den Lieferanten von allen Ansprüchen frei, die von Dritten, einschließlich Aufsichtsbehörden, geltend gemacht werden, wenn durch die Nutzung der Datensätze der öffentlichen Einrichtung Rechte des geistigen Eigentums, Datenschutzrechte oder gleichwertige Rechte verletzt wurden.

## Abschnitt E – KI-Register und Audit

Mit Ausnahme von Art. 20.1 gelten die Regelungen dieses Abschnitts nur bei einem Hochrisiko-System nach Art. 6 KI-VO.

### Artikel 19      <Fakultativ> KI-Register

- 19.1. 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.
- 19.2. Die öffentliche Einrichtung ist berechtigt, die in Artikel 19 Absatz 1 dargelegten Informationen an Dritte weiterzugeben und beispielsweise in einem Register für KI-Systeme zu veröffentlichen.
- 19.3. Auf Verlangen der öffentlichen Einrichtung ist der Lieferant bei der Eintragung der KI-Systeme in ein entsprechendes Register behilflich.

### Artikel 20      Einhaltung der Bestimmungen und Audit

- 20.1. Auf erstes Ersuchen der öffentlichen Einrichtung muss der Lieferant der öffentlichen Einrichtung alle Informationen zur Verfügung stellen, die für den Nachweis der Einhaltung dieser Anlage erforderlich sind.
- 20.2. 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 dieser Anlage 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.
- 20.3. 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.
- 20.4. Die öffentliche Einrichtung ist berechtigt, die Ergebnisse des in Artikel 20 Absatz 3 genannten Berichts gegenüber zuständigen Behörden zu veröffentlichen.
- 20.5. Die öffentliche Einrichtung ist berechtigt, einmal pro Kalenderjahr oder im Zusammenhang mit einer wesentlichen Änderung ein Audit durchzuführen oder durchführen zu lassen.

## Anlage Nr. 06 – KI-Mustervertragsklauseln

- 20.6. Die öffentliche Einrichtung kann beschließen, das Audit ganz oder teilweise von einem unabhängigen Prüfer durchführen zu lassen.
- 20.7. 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 Anlage** auszusetzen. Die öffentliche Einrichtung muss keine Gebühr zahlen, wenn das Audit ergibt, dass der Lieferant seinen Pflichten im Rahmen dieser **Anlage** nicht nachgekommen ist.

### Abschnitt F – Kosten

#### Artikel 21      Kosten

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

## Anhang A – Das KI-System und die Zweckbestimmung

Dieser Anhang wird im Vertrag individuell vereinbart und integraler Bestandteil der KI-Mustervertragsklauseln zu diesem Vertrag.

### Beschreibung des KI-Systems

In den Geltungsbereich der KI-Mustervertragsklauseln zu diesem Vertrag 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

Dieser Anhang wird im Vertrag individuell vereinbart und integraler Bestandteil der KI-Mustervertragsklauseln zu diesem Vertrag.

*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 <sup>2</sup>
		Ja/Nein
		Ja/Nein
		Ja/Nein

<sup>2</sup> 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 14 beschriebenen Pflichten des Lieferanten.



## Anlage Nr. 06 – KI-Mustervertragsklauseln

		Ja/Nein
--	--	---------

## Anhang C – Technische Dokumentation

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

1. allgemeine Beschreibung des KI-Systems, einschließlich folgender Angaben:
  - 1.1. Zweckbestimmung, Name des Lieferanten und Version des Systems mit Angaben dazu, in welcher Beziehung sie zu vorherigen Versionen steht,
  - 1.2. gegebenenfalls Interaktion oder Verwendung des KI-Systems mit Hardware oder Software, einschließlich anderer KI-Systeme, die nicht Teil des KI-Systems selbst sind,
  - 1.3. Versionen der betreffenden Software oder Firmware und etwaige Anforderungen in Bezug auf Aktualisierungen der Versionen,
  - 1.4. Beschreibung der Hardware, auf der das KI-System betrieben werden soll,
  - 1.5. falls das KI-System Bestandteil von Produkten ist: Fotografien oder Abbildungen, die äußere Merkmale, Kennzeichnungen und den inneren Aufbau dieser Produkte zeigen,
  - 1.6. eine grundlegende Beschreibung der Benutzerschnittstelle, die der öffentlichen Einrichtung zur Verfügung gestellt wird,
  - 1.7. Betriebsanleitungen für den Betreiber und gegebenenfalls eine grundlegende Beschreibung der Benutzerschnittstelle,
  - 1.8. Informationen aus dem KI-Steckbrief der öffentlichen Einrichtung
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, Beschreibung der erwarteten Ausgabe des Systems und der erwarteten Qualität dieser Ausgabe, Entscheidungen über mögliche Kompromisse in Bezug auf die technischen Lösungen, mit denen die Anforderungen nach **dieser Anlage** 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, einschließlich einer allgemeinen Beschreibung dieser Datensätze sowie Informationen zu deren Herkunft, Umfang und Hauptmerkmalen, Angaben zur Beschaffung und Auswahl der Daten; Kennzeichnungsverfahren (z. B. für überwachtes Lernen), Datenbereinigungsmethoden (z. B. Erkennung von Ausreißern),
- 2.5. Bewertung der gemäß **dieser Anlage** erforderlichen Maßnahmen der menschlichen Aufsicht, mit einer Bewertung der technischen Maßnahmen, die erforderlich sind, um der öffentlichen Einrichtung gemäß **dieser Anlage** die Interpretation der Ausgaben von KI-Systemen zu erleichtern,
  - 2.6. 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 **dieser Anlage** weiterhin dauerhaft erfüllt,
  - 2.7. verwendete Validierungs- und Testverfahren, mit Angaben zu den verwendeten Validierungs- und Testdaten und deren Hauptmerkmalen, Parameter, die zur Messung der Genauigkeit, Robustheit und der Erfüllung anderer einschlägiger Anforderungen nach **dieser Anlage** 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,
  - 2.8. Angaben zu ergriffenen Cybersicherheitsmaßnahmen,
3. 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,
  4. Darlegungen zur Eignung der Leistungskennzahlen für das KI-System,
  5. detaillierte Beschreibung des Risikomanagementsystems gemäß Artikel 2,
  6. 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, einschließlich diesbezüglicher Metriken, 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 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. gegebenenfalls die technischen Fähigkeiten und Merkmale des KI-Systems, um Informationen bereitzustellen, die zur Erläuterung seiner Ausgaben relevant sind,
  - 2.5. gegebenenfalls seine Leistung in Bezug auf bestimmte Personen oder Personengruppen, auf die das KI-System bestimmungsgemäß angewandt werden soll,
  - 2.6. gegebenenfalls die Spezifikationen für die Eingabedaten oder sonstige relevante Informationen über die verwendeten Trainings-, Validierungs- und Testdatensätze unter Berücksichtigung der Zweckbestimmung des KI-Systems,
  - 2.7. gegebenenfalls Informationen, die es der öffentlichen Einrichtung ermöglichen, die Ausgabe des KI-Systems zu interpretieren und sie angemessen zu nutzen,
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 Ausgaben des KI-Systems zu erleichtern,
5. die erforderlichen Rechen- und Hardware-Ressourcen, die erwartete Lebensdauer des KI-Systems und alle erforderlichen Wartungs- und Pflegemaßnahmen

## Anlage Nr. 06 – KI-Mustervertragsklauseln

einschließlich deren Häufigkeit zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates,

6. gegebenenfalls eine Beschreibung der in das KI-System integrierten Mechanismen, die es der öffentlichen Einrichtung ermöglicht, die Protokolle im Einklang mit Artikel 5 dieser **Anlage** ordnungsgemäß zu erfassen, zu speichern und auszuwerten.

## **Anhang E – Maßnahmen zur Gewährleistung der Transparenz**

Dieser Anhang wird im Vertrag individuell vereinbart und integraler Bestandteil der KI-Mustervertragsklauseln zu diesem Vertrag.

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

## **Anhang F – Maßnahmen zur Gewährleistung der menschlichen Aufsicht**

Dieser Anhang wird im Vertrag bei Bedarf individuell vereinbart und integraler Bestandteil der der KI-Mustervertragsklauseln zu diesem Vertrag.

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



## **Anhang G – Genauigkeitsgrade**

Dieser Anhang wird im Vertrag individuell vereinbart und integraler Bestandteil der KI-Mustervertragsklauseln zu diesem Vertrag.

*Bitte beschreiben Sie hier die erforderlichen Genauigkeitsgrade.*

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

Dieser Anhang wird im Vertrag individuell vereinbart und integraler Bestandteil der KI-Mustervertragsklauseln zu diesem Vertrag.

*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 **Anlage** 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 Versuchen unbefugter Dritter sein, seine Verwendung, sein Verhalten, seine Ausgaben 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, Erwidern, 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.*