ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Technische Dokumentation nach CRA, KI-VO und DSGVO

Vorlage für eine rechtsaktübergreifende technische Dokumentation

AUTOREN

Ceyda Özdemir
Fraunhofer SIT, ATHENE und HNFIZ 7

Sarah Stummer
Fraunhofer SIT, ATHENE und HNFIZ 7

Impressum

Kontakt
Nationales Forschungszentrum für angewandte
Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Die vorliegenden Ergebnisse sind im Rahmen des Fraunhofer Heilbronn Forschungs- und Innovationszentrums Cybersicherheit, das durch die Dieter Schwarz Stiftung gefördert wird, entstanden. Dieser Beitrag wurde zudem vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Inhalt

Einleitung

Die vorliegende Dokumentationsvorlage bietet eine gemeinsame Struktur für die technische Dokumentation nach der Verordnung über künstliche Intelligenz (KI-VO), dem Cyber Resilience Act (CRA) und der Datenschutz-Grundverordnung (DSGVO).

Sie eignet sich für Organisationen, die Hochrisiko-KI-Systeme gemäß der KI-VO in Verkehr bringen, die in ihrer Gesamtheit als Produkte mit digitalen Elementen (nachfolgend: Produkte) im Sinne des CRA einzustufen sind, bei der Entwicklung oder im späteren Wirkbetrieb zugleich mit einer Verarbeitung personenbezogener Daten im Sinne der DSGVO einhergehen und für die daher nach allen drei Rechtsakten (technische) Dokumentationspflichten bestehen.

Durch eine transparente Darstellung der jeweiligen Rechtsgrundlagen zu Beginn eines jeden Kapitels sowie ggf. auf Ebene der einzelnen zu beschreibenden Inhalte, lässt sich die Vorlage beliebig an die eigenen Rahmenbedingungen anpassen und in leicht veränderter Fassung verwenden – z.B. auch für eine gemeinsame technische Dokumentation nach KI-VO und CRA (und nicht nach DSGVO).

1. Allgemeine Beschreibung

1.1 Zweckbestimmung

Rechtsgrundlagen: Anhang IV (1a) KI-VO; Anhang VII (1a) CRA; Art. 25, 32, Erwägungsgrund 76 DSGVO

Inhalte:

- Verwendungszweck des Hochrisiko-KI-Systems/Produkt: Erläuterung der vorgesehenen Funktionen des Hochrisiko-KI-Systems/Produkts (z.B. Analyse, Klassifikation oder Steuerungsaufgaben) und des übergeordneten Zwecks, den das Hochrisiko-KI-System/Produkt erfüllen soll. Ggf. auch Darstellung der Kontexte, in denen das Hochrisiko-KI-System/Produkt eingesetzt wird, z.B. industrielle Steuerung oder Kundeninteraktion.
  (Rechtsgrundlagen: Anhang IV (1a) KI-VO; Anhang VII (1a) CRA)
- Verarbeitung personenbezogener Daten: Beschreibung von Art, Umfang, Umständen und Zwecken der Datenverarbeitung. Hierzu zählen Angaben zu den verarbeiteten Daten und deren Umfang (Sensordaten, Textdaten, Bilddaten etc.), zum Umfang der Verarbeitung selbst (z.B. bloße Speicherung oder auch Weiterleitung, Anordnung, etc.), zu den Kategorien betroffener Personen (z.B. Beschäftigte oder Kunden) und zu den konkreten Zwecken, die mit der Verarbeitung verbunden sind (z.B. Analyse der Eingabe- und Nutzungsdaten der verschiedenen Nutzer des Hochrisiko-KI-Systems/ Produkts mit digitalen Elementen zur Personalisierung von Inhalten).
  (Rechtsgrundlagen: Art. 25, 32, Erwägungsgrund 76 DSGVO)
- Anbieter des Hochrisiko-KI-Systems im Sinne des Art. 3 Nr. 3 KI-VO: Angabe der Stelle, von der das Hochrisiko-KI-System entwickelt wird bzw. die die Entwicklung beauftragt, und das Hochrisiko-KI-System unter eigenen Namen/eigener Handelsmarke in den Verkehr bringt oder in Betrieb nimmt.
  (Rechtsgrundlage: Anhang IV (1a) KI-VO)

1.2 Aufbau des Systems

Rechtsgrundlagen: Anhang IV (1b), (1c), (1e), (1f), (2c), (6) KI-VO; Anhang VII (1c), (2a) CRA

Inhalte:

- Visuelle Darstellung des Aufbaus: Fotografien, Illustrationen oder schematische Zeichnungen des Hochrisiko-KI-Systems/Produkts, einschließlich der äußeren Merkmale, Kennzeichnungen und ggf. interner Komponenten.
  (Rechtsgrundlagen: Anhang IV (1f) KI-VO; Anhang VII (1c) CRA)
- Systemarchitektur und Interaktionen: Beschreibung der Hierarchie und des Zusammenwirkens der einzelnen Komponenten und deren Integration in die Gesamtverarbeitung, ggf. unter Verwendung von Zeichnungen und Schemata. Beschreibung der Interaktion des Hochrisiko-KI-Systems/Produkts mit Hard- oder Software.
  (Rechtsgrundlagen: Anhang IV (2c), (1b) KI-VO; Anhang VII (2a) CRA)

- Hardware: Beschreibung der Hardware, auf der das Hochrisiko-KI-System betrieben werden soll.
  (Rechtsgrundlage: Anhang IV (1e) KI-VO)
- Änderungen im Lebenszyklus: Dokumentation aller relevanten Anpassungen, Updates und Verbesserungen, die den Betrieb oder die Leistung des Hochrisiko-KI-Systems beeinflussen, mit Zuordnung zu den Entwicklungs- oder Betriebsphasen.
  (Rechtsgrundlage: Anhang IV (6) KI-VO)
- Software- und Firmware-Voraussetzungen: Angaben zu den Versionen relevanter Software- und Firmware-Komponenten und zu Anforderungen an künftige Updates.
  (Rechtsgrundlagen: Anhang IV (1c) KI-VO)

1.3 Beschreibung der Benutzerschnittstelle

Rechtsgrundlagen: Anhang IV (1g), (1h) KI-VO

Beschreibung der grundlegenden Benutzerschnittstelle, die dem Betreiber des Hochrisiko-KI-Systems zur Verfügung gestellt wird.

1.4 Bereitstellungsformen

Rechtsgrundlage: Anhang IV (1d) KI-VO

Beschreibung der Bereitstellungsformen des Hochrisiko-KI-Systems: Bereitstellung, z.B. als in Hardware eingebettetes Softwarepaket oder als extern nutzbare API.

1.5 Unterstützungszeitraum und maßgebliche Faktoren

Rechtsgrundlage: Anhang VII (4) CRA

Inhalte:

- Unterstützungszeitraum: Darstellung des Zeitraums im Sinne des Art. 3 Nr. 20 CRA, in dem das Produkt Sicherheitsupdates, technische Unterstützung und Kompatibilitätsanpassungen erhält, z.B. 5 Jahre ab Inverkehrbringen.
- Begründung für die Wahl des Unterstützungszeitraums: Beschreibung der Einflussfaktoren wie Produktdetails, Marktverfügbarkeit, technologischer Fortschritt oder regulatorische Änderungen, welche den gewählten Unterstützungszeitraum beeinflusst haben.

1.6 System- oder Softwareversionen

Rechtsgrundlagen: Anhang IV (1a) KI-VO; Anhang VII (1b) CRA

Inhalte:

- Versionshistorie des Hochrisiko-KI-Systems: Angabe der Version des Hochrisiko-KI-Systems im Verhältnis zu vorherigen Versionen, um die Entwicklung, Änderungen und Übergänge zwischen den Versionen nachvollziehbar zu machen.
  (Rechtsgrundlage: Anhang IV (1a) KI-VO)

- Versionen der Software: Angabe der Versionen für Software, die für die Einhaltung der grundlegenden Cybersicherheitsanforderungen relevant sind. Umfasst ist hiervon sowohl das Softwareprodukt selbst (wenn es sich um ein Softwareprodukt handelt) als auch die darin enthaltenen Software-Komponenten. Relevant für die Einhaltung der grundlegenden Cybersicherheitsanforderungen können z.B. Authentifizierungs-, Verschlüsselungs- oder Intrusion-Detection-Mechanismen sein.
  (Rechtsgrundlage: Anhang VII (1b) CRA)

2. Beschreibung des Entwicklungsprozesses

2.1 Entwicklungsmethoden und -schritte

Rechtsgrundlage: Anhang IV (2a) KI-VO

Beschreibung der angewandten Entwicklungsmethoden und -schritte: Darstellung der Methoden und Schritte zur Entwicklung des Hochrisiko-KI-Systems, ggf. auch unter Einsatz von vortrainierten Systemen oder Instrumenten Dritter, ggf. auch in veränderter Form.

2.2 Entwurfsspezifikationen

Rechtsgrundlage: Anhang IV (2b) KI-VO

Inhalte:

- Allgemeine Logik des Hochrisiko-KI-Systems: Erläuterung der allgemeinen Logik des Hochrisiko-KI-Systems und der verwendeten Algorithmen.
- Wesentliche Designentscheidungen: Darstellung der getroffenen Entscheidungen, der zugrundeliegenden Annahmen und der Begründung dieser Entscheidungen, insbesondere in Bezug auf Personen oder Gruppen, durch welche die Verwendung des Hochrisiko-KI-Systems vorgesehen ist.
- Kompromisse bei technischen Lösungen: Angaben zu den getroffenen Entscheidungen über mögliche Kompromisse, die in Bezug auf die technischen Lösungen zur Einhaltung der Anforderungen an Hochrisiko-KI-Systeme nach Kapitel III Abschnitt 2 KI-VO getroffen wurden.
- Hauptklassifikationsentscheidungen: Dokumentation der Entscheidungen, die darüber bestimmen, wie das Hochrisiko-KI-System Kategorien bildet bzw. Entscheidungen oder Vorhersagen vornimmt.
- Optimierungsziele des Hochrisiko-KI-Systems: Falls das Hochrisiko-KI-System etwas optimieren soll, eine Darstellung des Optimierungsgegenstands und welche Relevanz die hierzu verwendeten Parameter haben.
- Erwartete Systemausgabe und -qualität: Erläuterung der erwarteten Ausgabe des Hochrisiko-KI-Systems sowie deren Qualität.

2.3 Informationen zu Trainingsdaten und Daten-Governance

Rechtsgrundlage: Anhang IV (2d) KI-VO

Inhalte:

- Datenanforderungen: Angaben zu Datenblättern, die die Trainingsmethoden, Techniken und verwendeten Datensätze beschreiben, einschließlich allgemeiner Beschreibung, Herkunft, Umfang und wesentlicher Merkmale der Datensätze.
- Datenbeschaffung und -auswahl: Darstellung, wie die Daten gewonnen und ausgewählt wurden.
- Kennzeichnungs- und Bereinigungsverfahren: Beschreibung der Verfahren zur Kennzeichnung der Kategorisierung durch das Hochrisiko-KI-System (Labelung, z.B. für überwachte Lernverfahren) und der Methoden zur Datenbereinigung (z.B. die Erkennung von Ausreißern).

2.4 Änderungen, Validierung und Testverfahren

Rechtsgrundlagen: Anhang IV (2f), (2g), (4) KI-VO

Inhalte:

- Vorab bestimmte Änderungen: Beschreibung der vorab festgelegten Änderungen und Maßnahmen zur Einhaltung regulatorischer Anforderungen.
  (Rechtsgrundlage: Anhang IV (2f) KI-VO)
- Validierungs- und Testverfahren: Erläuterung der eingesetzten Methoden und Informationen zu den verwendeten Test- und Validierungsdaten und deren wesentlichen Merkmalen.
  (Rechtsgrundlage: Anhang IV (2g) KI-VO)
- Leistungsmetriken und deren Eignung: Angabe der Kennzahlen zur Messung von Genauigkeit, Robustheit und zur Einhaltung weiterer relevanter Anforderungen, einschließlich möglicher diskriminierender Auswirkungen und Erläuterung, warum die gewählten Leistungsmetriken angemessen sind, um Genauigkeit, Robustheit und Einhaltung regulatorischer Anforderungen zu messen.
  (Rechtsgrundlage: Anhang IV (2g), (4) KI-VO)
- Testprotokolle und Berichte: Alle Testprotokolle und datierte sowie unterzeichnete Testberichte, insbesondere im Zusammenhang mit den vorab bestimmten Änderungen am Hochrisiko-KI-System, werden im Anhang dieser Dokumentation bereitgestellt.
  (Rechtsgrundlage: Anhang IV (2g) KI-VO)

2.5 Rechenressourcen

Rechtsgrundlage: Anhang IV (2c) KI-VO

Beschreibung der eingesetzten Rechenressourcen: Information über Ressourcen, die für Entwicklung, Training, Test und Validierung des Hochrisiko-KI-Systems genutzt werden.

2.6 Einbindung datenschutzrechtlicher Vorgaben in die Entwicklung

Rechtsgrundlagen: Art. 25, 32 DSGVO

Inhalte:

- Datenschutz im Entwicklungsprozess: Beschreibung, wie die datenschutzrechtlichen Anforderungen beim Entwicklungs- und Konzeptionsprozess einbezogen wurden, insbesondere der Grundsatz der Rechtmäßigkeit, Zweckbindung und Datenminimierung (z.B. beim Training des Hochrisiko-KI-Systems mit personenbezogenen Daten).
  (Rechtsgrundlage: Art. 25 DSGVO)
- Datensicherheit im Entwicklungsprozess: Beschreibung der Risiken, die durch die Verarbeitung personenbezogener Daten während der Konzeptions- und Entwicklungsphase (z.B. beim Training des Hochrisiko-KI-Systems mit personenbezogenen Daten) für die Rechte und Freiheiten natürlicher Personen und Beschreibung der technischen und organisatorischen Maßnahmen, die ergriffen wurden, um den Risiken im Zusammenhang mit der Datensicherheit zu begegnen.
  (Rechtsgrundlage: Art. 32 DSGVO)
- Datenschutz durch Technikgestaltung: Beschreibung der technischen und organisatorischen Maßnahmen, die ergriffen wurden, um das Hochrisiko-KI-System/ Produktdatenschutzkonform zu gestalten.
  (Rechtsgrundlage: Art. 25 DSGVO)
- Datenschutzfreundliche Voreinstellungen: Beschreibung der Standardkonfiguration des Hochrisiko-KI-Systems/Produkts, die sicherstellt, dass nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet werden.
  (Rechtsgrundlage: Art. 25 DSGVO)

3. Risikomanagement

3.1 Risikoidentifikation

Rechtsgrundlagen: Anhang IV (5), Art. 9 KI-VO; Art. 32 DSGVO; Anhang VII (3), Art. 13 CRA

Beschreibung der Risiken, die beim künftigen Einsatz des Hochrisiko-KI-Systems/Produkts für die Cybersicherheit (CRA), die Gesundheit, Sicherheit oder Grundrechte (KI-VO) und/oder für die Rechte und Freiheiten natürlicher Personen (DSGVO) bestehen.

Risiken	**KI-VO** Risiko für Gesundheit, Sicherheit oder Grundrechte	**CRA** Risiko für Cybersicherheit	**DSGVO** Risiko für Rechte und Freiheiten natürlicher Personen
Risiko 1	☐	☐	☐
Risiko 2	☐	☐	☐
Risiko 3	☐	☐	☐
…	☐	☐	☐

3.2 Risikobewertung

Rechtsgrundlagen: Anhang IV (5), Art. 9 KI-VO; Art. 32 DSGVO; Anhang VII (3), Art. 13 CRA

Inhalte:

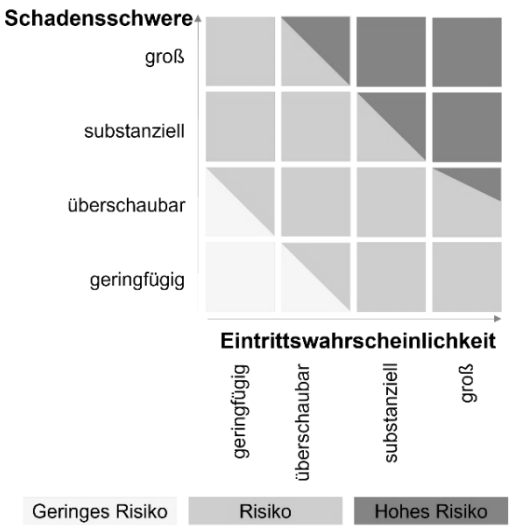
- Einzelrisiken: Bewertung der Eintrittswahrscheinlichkeit und Schadensschwere der einzelnen, identifizierten Risiken anhand der Abstufungen *geringfügig*, *überschaubar*, *substanziell* und *groß* sowie Bewertung der Einzelrisiken anhand einer definierten Risikomatrix.
- Gesamtrisiko: Bewertung des Gesamtrisikos nach CRA, KI-VO und DSGVO anhand einer definierten Risikomatrix. Maßgeblich ist das Einzelrisiko mit der höchsten Einzelrisikobewertung, das je Rechtsakt einschlägig ist.

Risiken	Eintrittswahr-scheinlichkeit	Schadens-ausmaß	Einzel-risiko
Risiko 1			
Risiko 2			
Risiko 3			
…			

Gesamtrisiko nach CRA:
☐ gering ☐ normal ☐ hoch

Gesamtrisiko nach KI-VO:
☐ gering ☐ normal ☐ hoch

Gesamtrisiko nach DSGVO:
☐ gering ☐ normal ☐ hoch



3.3 Maßnahmenauswahl und -umsetzung

Rechtsgrundlagen: Anhang IV (2h), Art. 9 KI-VO; Art. 32 DSGVO; Anhang VII (3) CRA

Beschreibung der technischen und organisatorischen Maßnahmen, inklusive Cybersicherheitsmaßnahmen, die getroffen wurden, um den identifizierten Risiken zu begegnen.

3.4 Restrisikobewertung

Rechtsgrundlagen: Anhang IV (5), Art. 9 KI-VO, Art. 35 DSGVO

Prüfung, ob die Einzel- und Gesamtrestrisiken, die nach Umsetzung der Maßnahmen verbleiben, als vertretbar eingestuft werden können sowie eine Begründung. Als vertretbar einzustufen sind die verbleibenden Einzel- und Gesamtrestrisiken, wenn nach der Umsetzung der Maßnahmen weder die verbleibenden Einzelrisiken noch die verbleibenden Gesamtrisiken als hoch einzustufen sind.

3.5 Risiko-Monitoring und Aktualisierung

Rechtsgrundlagen: Anhang IV (5), Art. 9 KI-VO; Art. 32 DSGVO; Anhang VII (3), Art. 13 CRA

Inhalte:

- Technisches Monitoring: Erläuterung, wie das technische Monitoring erfolgt und Anpassungsbedarf erkennt, z.B. durch eine Auswertung der Ausfälle, Angriffe oder technischen Fehlern.
- Organisatorisches Monitoring: Erläuterung, in welchen Intervallen und bei welchen Anlässen die identifizierten Risiken und die Wirksamkeit der implementierten Maßnahmen überprüft werden und welche Parteien an dieser Überprüfung beteiligt sind.
- Änderungen während des Lebenszyklus: Auflistung aller Änderungen des Risikomanagementsystems, die während des Lebenszyklus des Hochrisiko-KI-Systems/Produkts erfolgt sind.

4. Überwachungsprozesse

4.1 Herstellungs- und Überwachungsprozesse

Rechtsgrundlage: Anhang VII (2c) CRA

Inhalte:

- Herstellungs- und Überwachungsprozesse: Notwendige Informationen und Spezifikationen der Herstellungs- und Überwachungsprozesse des Produkts.
- Validierung der Prozesse: Darstellung, wie die Produktions- und Überwachungsprozesse validiert und ihre Funktionsfähigkeiten überprüft werden.

4.2 Überwachung der Fähigkeiten, Leistungsgrenzen und unbeabsichtigte Risiken

Rechtsgrundlage: Anhang IV (3) KI-VO

Beschreibung von Überwachung, Funktion und Kontrolle des Hochrisiko-KI-Systems: Detaillierte Informationen darüber, wie das Hochrisiko-KI-System in Bezug auf seine Fähigkeiten und Leistungsgrenzen, inklusive seiner Genauigkeitsgrade, sowie in Bezug auf vorhersehbare unbeabsichtigte Ergebnisse und Quellen von Risiken überwacht und kontrolliert wird. Ggf. Angaben zu den verwendeten Eingabedaten, sofern relevant für die Überwachung.

4.3 Menschliche Aufsicht

Rechtsgrundlagen: Anhang IV (2e), (3) KI-VO

Maßnahmen zur menschlichen Aufsicht: Darstellung der Maßnahmen nach Art. 14 KI-VO, die getroffen wurden, um Hochrisiko-KI-System Betreibern im Sinne des Art. 3 Nr. 4 KI-VO die Interpretation der Systemausgaben zu erleichtern, sowie eine Begründung.

4.4 System zur Bewertung der Leistung nach dem Inverkehrbringen

Rechtsgrundlage: Anhang IV (9) KI-VO

Inhalte:

- System zur Bewertung der Leistung des Hochrisiko-KI-Systems in der Post-Market-Phase: Detaillierte Beschreibung der eingesetzten Verfahren zur Evaluierung der Systemleistung nach der Markteinführung gemäß Art. 72 KI-VO.
- Post-Market-Monitoring-Plan: Darstellung des Überwachungsplans nach Art. 72 Abs. 3 KI-VO, einschließlich der vorgesehenen Schritte zur kontinuierlichen Beobachtung und Bewertung des Hochrisiko-KI-Systems im Betrieb.

5. Schwachstellenmanagement

Rechtsgrundlage: Anhang VII (2b) CRA

Inhalte:

- Prozesse zur Behandlung von Schwachstellen: Darstellung, wie Schwachstellen identifiziert, bewertet und behoben werden, um die Einhaltung der grundlegenden Cybersicherheitsanforderungen aus Teil I und II des Anhangs I CRA sicherzustellen. Angabe, ob und in welchem Umfang eine Software-Stückliste erstellt wurde und inwieweit sie bei der Behandlung von Schwachstellen hilft. Sofern die Marktüberwachungsbehörde dies verlangt oder der Hersteller es für interne Zwecke für sinnvoll erachtet, wird die Software-Stückliste im Anhang dieser Dokumentation bereitgestellt.
- Koordinierte Offenlegung von Schwachstellen: Darstellung, wie Schwachstellen offengelegt werden.
- Kontaktadresse für die Meldung von Schwachstellen: Erläuterung und Nachweis, wo die Kontaktadresse zur Meldung von Schwachstellen bereitgestellt wird (z.B. Screenshot und Verlinkung).
- Updatemechanismen: Erläuterung der technischen Lösungen, die ergriffen wurden, um eine sichere Verbreitung von Aktualisierungen zu gewährleisten.

6. Einhaltung der Vorschriften

6.1 Berichte und Tests für Konformitätsprüfung

Rechtsgrundlage: Anhang VII (6) CRA

Test- und Prüfberichte: Dokumentation der Tests und Prüfungen, die durchgeführt wurden, um die Konformität des Produkts und der Verfahren zur Behandlung von Schwachstellen mit den geltenden grundlegenden Cybersicherheitsanforderungen aus Teil I und II des Anhangs I CRA zu überprüfen.

Die vollständigen Test- und Prüfberichte werden im Anhang dieser Dokumentation bereitgestellt.

6.2 Harmonisierte Normen und alternative Lösungen

Rechtsgrundlagen: Anhang IV (7) KI-VO; Anhang VII (5) CRA

Inhalte:

- Angewandte harmonisierten Normen nach KI-VO oder alternativen Lösungen: Auflistung der vollständigen oder teilweise angewandten harmonisierten Normen, deren Referenzen im Amtsblatt der Europäischen Union veröffentlicht wurden. Falls keine solchen harmonisierten Normen angewandt wurden, Beschreibung der Lösungen, einschließlich einer Auflistung weiterer relevanter Normen und technischer Spezifikationen, die zur Erfüllung der Anforderungen aus Kapitel III Abschnitt 2 KI-VO angewendet wurden.
- Angewandte harmonisierte Normen, Spezifikationen und Schemata nach CRA oder alternativen Lösungen: Aufstellung der vollständigen oder teilweise angewandten harmonisierten Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, der in Art. 27 CRA genannten gemeinsamen Spezifikationen oder der in Art. 27 Abs. 8 CRA genannten europäischen Schemata für die Cybersicherheitszertifizierung, angenommen gemäß der Verordnung (EU) 2019/881.Ggf. unter Angabe, welche Teile angewandt wurden. Falls solche nicht angewandt wurden, Beschreibung der Lösungen, mit denen die grundlegenden Cybersicherheitsanforderungen aus Teil I und II des Anhangs I CRA erfüllt werden.

6.3 EU-Konformitätserklärung

Rechtsgrundlagen: Anhang IV (8) KI-VO; Anhang VII (7) CRA

Die unterzeichneten EU-Konformitätserklärungen sind dem Anhang dieser Dokumentation beigefügt.

Anhang: Weiterführende Informationen

- (Link auf) Informationen und Anleitungen für die Nutzer gemäß Anhang II CRA
  (Rechtsgrundlage: Anhang VII (1d) CRA)
- (Link auf) Betriebsanleitung für Betreiber des Hochrisiko-KI-Systems
  (Rechtsgrundlage: Anhang VII (1h) KI-VO)
- *Sofern die Marktüberwachungsbehörde dies verlangt*: Software-Stückliste
  (Rechtsgrundlage: Anhang VII (8) CRA)
- Testprotokolle und -berichte
  (Rechtsgrundlage: Anhang IV (2g) KI-VO)
- Test- und Prüfberichte für Konformitätsprüfung des Produkts
  (Rechtsgrundlage: Anhang VII (6) CRA)
- EU-Konformitätserklärung des Produkts nach CRA
  (Rechtsgrundlage: Anhang VII (7) CRA)
- EU-Konformitätserklärung des Hochrisiko-KI-Systems nach KI-VO
  (*Rechtsgrundlage: Anhang IV (8) KI-VO)*