

Anlagen zum Vertragswerk Agentplattform „Agentic Microservices“

Anlage 1 bis Anlage 9 · gilt für die Online-Nutzungsbedingungen und für den Rahmenvertrag · Fassung 3.1,
Stand 30. September 2026

Inhalt

Anlage	Gegenstand
Anlage 1	Leistungsbeschreibung
Anlage 2	Preisliste
Anlage 3	Verfügbarkeit und Betreuung
Anlage 4	Vereinbarung zur Auftragsverarbeitung
Anlage 5	Technische und organisatorische Maßnahmen
Anlage 6	Nutzungsrichtlinie und Überlassung von Rechenleistung
Anlage 7	Betrieb auf Systemen des Kunden, sofern vereinbart
Anlage 8	Datenpartnerschaft, nur bei gesonderter Zustimmung
Anlage 9	Hochrisiko-Agenten, nur bei Buchung eines Hochrisiko-Agenten

Diese Anlagen gelten unverändert für den Online-Abschluss und für den unterschriebenen Rahmenvertrag. Jede Anlage trägt eine eigene Fassungsnummer; maßgeblich ist die in der Bestellung oder im Leistungsschein genannte Fassung.

Anlage 1 – Leistungsbeschreibung

Diese Anlage beschreibt die geschuldete Leistung abschließend. Was hier nicht steht, ist nicht geschuldet.

1. Gegenstand der Plattform

- [Zulieferung Technik: Kurzbeschreibung der Plattform – bewusst knapp, nur Kernfunktionen]
- [Zulieferung Technik: Bedienoberfläche: Ansichten, Funktionen, Rollen – bewusst knapp, nur Kernfunktionen]
- Die Plattform protokolliert Eingaben, Änderungen und Löschungen mit Benutzerkennung und Zeitstempel sowie die Freigaben nach § 8 Abs. 3 der Nutzungsbedingungen bzw. des Rahmenvertrags; Einzelheiten ergeben sich aus Anlage 5. Die Protokolle sind für die in Anlage 5 (Abschnitt „Aufbewahrungsfristen der Protokolle“) genannte Dauer einsehbar.
- Bei freigabepflichtigen Vorgängen nach § 8 Abs. 2 der Nutzungsbedingungen bzw. des Rahmenvertrags und nach dem Datenblatt des Agenten hält der Agent den Vorgang an, bis eine befugte Person des Kunden ihn freigibt. Die Freigabe wird mit Person und Zeitpunkt protokolliert (§ 8 Abs. 3).

2. Betriebsmodelle

Regelfall ist das Betriebsmodell A1. Der Anbieter beschafft die für den Betrieb erforderlichen Server und Grafikkarten auf eigene Rechnung, richtet sie ein und betreibt sie. Der Kunde muss selbst keine Hardware beschaffen und keinen Vertrag mit einem Rechenzentrum schließen. Wünscht der Kunde ausdrücklich, die Infrastruktur selbst anzumieten oder die Plattform auf eigenen Systemen zu betreiben, stehen ihm die Betriebsmodelle A2 und C offen.

Modell	Beschreibung	Verfügbar in
A1 – Beschaffung durch den Anbieter	Der Anbieter beschafft Server und Grafikkarten auf eigene Rechnung und betreibt die Plattform darauf. Abrechnung je Grafikkarte und angefangener Kalenderstunde nach Anlage 2. Regelfall.	Test, Business, Pro, Enterprise
A2 – Anmietung durch den Kunden	Auf ausdrücklichen Wunsch mietet der Kunde Server und Grafikkarten selbst an und ist Vertragspartner des Rechenzentrums. Der Anbieter erbringt die Leistungen nach Anlage 6 Ziffer 4 Abs. 2.	Enterprise; Business und Pro nur auf gesonderte Vereinbarung
C – On-Premise	Plattform und Modelle laufen vollständig auf Systemen des Kunden. Anlage 7.	Enterprise

Eine Grafikkarte trägt bis zu fünf gleichzeitig aktive Agenten. Der Bedarf an Grafikkarten richtet sich nach der Anzahl der aktivierten Agenten. Weitere Karten werden bei Bedarf zugeschaltet und in nachfrageschwachen Zeiten wieder abgeschaltet.

Technische Mindestanforderungen für die Betriebsmodelle A2 und C: [Zulieferung Technik: Grafikkarten, Speicher, Netz, Betriebssystem, Virtualisierung, Anforderungen an den Aufstellungsort]

Modellklassen. Die Plattform wird in Modellklassen angeboten. Eine Modellklasse wird nicht über den Namen eines Modells beschrieben, sondern über folgende Merkmale: Kontextlänge, unterstützte Sprachen, unterstützte Modalitäten, Latenzband je Vorgang, Verarbeitungsort sowie die Angabe, ob ein vom Anbieter feinabgestimmtes Modell zum Einsatz kommt. Die angebotenen Klassen sind nachstehend beschrieben. Innerhalb der vereinbarten Klasse ist der Anbieter in der Wahl des Modells frei; die Merkmale der Klasse werden nicht unterschritten. Die je Paket zugeordnete Klasse ergibt sich aus Anlage 2 Ziffer 1.

Modellklasse 1 — Basis. Kontextlänge mindestens 32.000 Token; unterstützte Sprachen Deutsch und Englisch; Modalität Text; Latenzband je Vorgang im Median höchstens 60 Sekunden; Verarbeitungsort Europäische Union; ohne vom Anbieter feinabgestimmtes Modell.

Modellklasse 2 — Standard. Kontextlänge mindestens 128.000 Token; unterstützte Sprachen Deutsch, Englisch sowie Französisch, Italienisch, Spanisch und Niederländisch; Modalitäten Text und Dokumentbild mit Texterkennung; Latenzband je Vorgang im Median höchstens 30 Sekunden; Verarbeitungsort Europäische Union; ein vom Anbieter feinabgestimmtes Modell kann zum Einsatz kommen.

Modellklasse 3 — Erweitert. Kontextlänge mindestens 200.000 Token; unterstützte Sprachen wie Klasse 2 zuzüglich weiterer auf Anfrage; Modalitäten Text, Dokumentbild mit Texterkennung und strukturierte Daten; Latenzband je Vorgang im Median höchstens 15 Sekunden; Verarbeitungsort Europäische Union; **ein für den Kunden feinabgestimmtes Modell ist gegen gesonderte Vergütung nach Anlage 2 Ziffer 7 möglich.**

3. Systemvoraussetzungen und Übergabepunkt

(1) Übergabepunkt in den Betriebsmodellen A1 und A2 ist der Routerausgang des genutzten Rechenzentrums. Im Betriebsmodell C gibt es keinen Übergabepunkt; die Leistung ist mit Bereitstellung der Programmfassung erbracht.

(2) Voraussetzungen beim Kunden: **[Zulieferung Technik: unterstützte Browser und Versionen, Mindestbandbreite, Freigaben in der Firewall, benötigte Ports und Adressbereiche]**

(3) **Anlaufzeit.** Ist einem Agenten zum Zeitpunkt der Auslösung keine Grafikkarte zugeordnet, beginnt die Bearbeitung innerhalb von 10 Minuten. Innerhalb einer bereits angefangenen Kalenderstunde erfolgt die Bearbeitung ohne Anlaufzeit; eine angefangene Kalenderstunde bleibt bis zu ihrem Ende verfügbar.

4. Beschreibung der einzelnen Agenten

Für jeden beauftragten Agenten wird das nachfolgende Datenblatt ausgefüllt. Nicht beschriebene Agenten sind nicht Vertragsgegenstand.

Das Datenblatt ist zugleich die Information des Kunden als Betreiber nach dem Paragraphen zur Verordnung über künstliche Intelligenz. Es wird in der Verwaltungsoberfläche in der jeweils aktuellen Fassung bereitgehalten.

Datenblatt Agent Nr. ____

Feld	Angabe
Bezeichnung	[z. B. Eingangsrechnungen]
Bearbeiteter Vorgangstyp	[was genau ist ein Vorgang bei diesem Agenten]
Auslöser	[Posteingang, Zeitplan, manuelle Auslösung, Schnittstelle]
Eingangsdaten	[Formate, Quellen, Qualitätsanforderungen]
Arbeitsschritte	[Schritte in der Reihenfolge der Ausführung]
Ergebnis	[was gibt der Agent aus, in welchem Format, wohin]
Freigabepflichtig	[ja / nein; falls ja: welche Rolle gibt frei]
Ausdrücklich nicht geschuldet	[was der Agent nicht leistet]
Bekannte Grenzen	[typische Fälle, in denen der Agent scheitert oder eskaliert]
Eskalationsweg	[was passiert bei Unsicherheit oder Fehler]

Feld	Angabe
Angebundene Fremdsysteme	[Bezeichnung, Schnittstelle, wer stellt Zugänge]
Verarbeitete Datenkategorien	[verarbeitete Datenkategorien]
Betroffene Personengruppen	[betroffene Personengruppen, z. B. Beschäftigte, Kunden, Lieferanten, Bewerber]
Einstufung nach der KI-Verordnung	[kein Hochrisiko mit Begründung / Hochrisiko-Agent nach Anlage 9]
Anhang-III-Bereich und Zweckbestimmung (nur Hochrisiko-Agenten)	[Nr. 3, 4, 5 a, 5 b oder 5 c; Zweckbestimmung wie in der Betriebsanleitung und der EU-Konformitätserklärung]
Konformität (nur Hochrisiko-Agenten)	[Verfahren nach Art. 43; EU-Konformitätserklärung vom; CE-Kennzeichnung; Registriernummer in der EU-Datenbank]
Betriebsanleitung (nur Hochrisiko-Agenten)	[Fassung und Datum der Betriebsanleitung nach Anlage 9 Ziffer 3]
Modellklasse und Verarbeitungsort	[Modellklasse nach Abschnitt 2; Verarbeitungsort]
Menschliche Aufsicht	[an welchen Stellen der Lauf anhält, wer freigibt, wie ein Lauf abgebrochen wird; erforderliche KI-Kompetenz der beteiligten Personen]
Transparenz nach Art. 50 KI-VO	[ob der Agent mit Personen interagiert oder Inhalte erzeugt; wie Hinweis und Kennzeichnung umgesetzt sind; Pflichten des Kunden bei Veröffentlichung]
Typische Fehlerbilder	[häufige Fehler, woran sie erkennbar sind, wie zu reagieren ist]
Richtwert Vorgänge je Monat	[Zahl]

5. Einrichtung

- Business: 2 Stunden begleitete Einrichtung. Pro: 4 Stunden. Enterprise und Betriebsmodell C: nach Leistungsschein.
- In dieser Zeit erfolgen die Ersteinrichtung, die Anbindung eines Fremdsystems, ein Testlauf und eine Einweisung.
- Mehraufwand über diesen Umfang hinaus wird nach Aufwand zum Stundensatz nach Anlage 2 Ziffer 7 vergütet.

Die Einrichtung ist eine Dienstleistung. Ein bestimmter Erfolg ist nur bei ausdrücklicher Vereinbarung in Textform geschuldet.

6. Nicht geschuldete Leistungen

- die inhaltliche Richtigkeit einzelner Ergebnisse,
- Beschaffung, Pflege und Verfügbarkeit von Fremdsystemen des Kunden,
- Bereinigung und Pflege der Datenbestände des Kunden,
- rechtliche, steuerliche oder sonstige berufsrechtlich gebundene Beratung,
- Archivierung im Sinne handels- und steuerrechtlicher Aufbewahrungspflichten,
- im Betriebsmodell C: Betrieb, Verfügbarkeit, Sicherheit und Datensicherung der Systeme des Kunden,
- die Erfüllung der Pflichten des Kunden als Betreiber nach der Verordnung (EU) 2024/1689, insbesondere nach den Artikeln 26, 27 und 86,

- die Auslösung von Zahlungsaufträgen bei Zahlungsdienstleistern. Diese Funktion ist nicht Bestandteil der Plattform. Agenten bereiten Zahlungen vor; Freigabe und Auslösung erfolgen im System des Kunden. Richtet der Kunde eine Auslösung über eine von ihm selbst eingerichtete Anbindung ein, handelt er in eigener Verantwortung; die Freigabepflicht nach § 8 Abs. 2 bleibt unberührt,
- sowie die im Datenblatt des Agenten unter „Ausdrücklich nicht geschuldet“ genannten Leistungen.

Anlage 2 – Preisliste

Fassung 3.0, 30. September 2026. Alle Preise in Euro, zuzüglich der gesetzlichen Umsatzsteuer.

1. Pakete in den Betriebsmodellen A1 und A2

Paket	Agenten	Entgelt je Monat	Richtwert Vorgänge
Test	3	199 einmalig, 30 Tage	rund 300
Business	5	490	rund 2.500
Pro	10	1.490	rund 5.000
Enterprise	25	ab 3.490	rund 12.500

Im Testpaket sind 40 Rechenstunden enthalten; Hochrisiko-Agenten nach Anlage 9 sind im Testpaket nicht verfügbar. Das einmalige Entgelt von 199 Euro wird auf den ersten Monat angerechnet, wenn der Kunde innerhalb von dreißig Kalendertagen nach Ende des Testzeitraums ein Paket beauftragt. Die Zahl der Nutzerzugänge ist in allen Paketen unbegrenzt. Die Angaben zu Vorgängen sind unverbindliche Orientierungswerte; sie begründen weder eine Mengenbegrenzung noch eine zugesicherte Leistungsmenge. Das Paketentgelt ist unabhängig von der Zahl der bearbeiteten Vorgänge zu zahlen.

Modellklasse je Paket: Test Modellklasse 1, Business Modellklasse 1, Pro Modellklasse 2, Enterprise Modellklasse 3. Der Wechsel in eine höhere Modellklasse ist zum Monatsersten möglich und wird mit 49 Euro je Agent und Monat vergütet. Die Merkmale der Klassen ergeben sich aus Anlage 1 Abschnitt 2.

2. Zusätzliche Agenten

Paket	Entgelt je Agent und Monat	Geltungsbereich
Business	199	ab dem 6. Agenten, ohne Obergrenze
Pro	139	ab dem 11. Agenten, ohne Obergrenze
Enterprise	100	ab dem 26. Agenten
Enterprise	89	ab dem 50. Agenten
Enterprise	79	ab dem 100. Agenten
On-Premise	149	ab dem 26. Agenten

Die Entgelte für zusätzliche Agenten gelten stufenweise: Jeder Agent wird mit dem Preis der Stufe berechnet, in die er fällt (im Paket Enterprise 100 Euro für den 26. bis 49. Agenten, 89 Euro für den 50. bis 99. Agenten und 79 Euro ab dem 100. Agenten).

3. Rechenleistung

Regelfall ist die Beschaffung durch den Anbieter. Er beschafft Server und Grafikkarten im eigenen Namen und auf eigene Rechnung und stellt dem Kunden die Rechenleistung zur Verfügung. Abgerechnet werden ausschließlich die tatsächlich erfassten Stunden. Eine Obergrenze der monatlichen Nutzung besteht nicht. Der Anbieter weist die Kosten offen aus: mit jeder Abrechnung nach Karten und Tagen gegliedert, laufend einsehbar in der Verwaltungsoberfläche und auf Verlangen quartalsweise durch Auskunft über die zugeordnete Kapazität.

Position	Preis	Hinweis
A1 – je Grafikkarte und angefangener	2,00	fester Preis je Karte und angefangener

Position	Preis	Hinweis
Kalenderstunde		Kalenderstunde
A1 – Obergrenze je Karte und Monat	keine	abgerechnet werden die Kalenderstunden mit Zuordnung
A2 – Entgelte des Rechenzentrums	trägt der Kunde unmittelbar	eigener Vertrag des Kunden
A2 – Verwaltungspauschale je Monat	[Betrag] 	Leistungen nach Anlage 6 Ziffer 4 Abs. 2
Dedizierte Hardware oder bestimmter Standort auf Wunsch	nach Angebot	gesonderte Vereinbarung
Reservierte Kapazität mit Mindestlaufzeit	nach Angebot	Restlaufzeit trägt der Kunde nach dem Vertrag

Eine Grafikkarte trägt bis zu fünf gleichzeitig aktive Agenten.

4. Betriebsmodell C – On-Premise

Position	Preis	Hinweis
Grundlizenz bis 25 Agenten, je Monat	4.990	Programmfassungen und Pflege enthalten
Je weiterem Agenten und Monat	149	ohne Obergrenze
Einmalige Bereitstellung und Inbetriebnahme	nach Angebot	einschließlich Installation und Abnahme
Fernwartungspaket, je Monat	nach Leistungsschein	optional, gesonderte Vereinbarung
Mindestlaufzeit	12 Monate	Verlängerung um jeweils zwölf Monate

5. Nachlässe bei Vorauszahlung

Zahlungsweise	Nachlass auf die monatlichen Entgelte	Bindung
Monatlich	kein Nachlass	monatlich kündbar
Vierteljährlich im Voraus	6 %	feste Laufzeit von drei Monaten
Jährlich im Voraus	16 %	feste Laufzeit von zwölf Monaten

Der Nachlass gilt nur für die monatlichen Entgelte nach den Ziffern 1, 2, 4 und 8. Rechenstunden werden stets ohne Nachlass abgerechnet.

6. Nachlass für die Datenpartnerschaft nach Anlage 8

Stufe	Nachlass auf die monatlichen Entgelte
Stufe 3 – Allgemeine Modellentwicklung	15 %

Der Nachlass wird ab dem auf die Zustimmung folgenden Abrechnungszeitraum gewährt und entfällt mit Wirkung für die Zukunft, sobald der Kunde die Teilnahme widerruft. Er ist mit den Nachlässen nach Ziffer 5 kumulierbar.

7. Weitere Leistungen

Leistung	Preis
Einrichtung über den Umfang der Anlage 1 hinaus, je Stunde	249
Schulung, je Stunde	249
Wechsel des Betriebsmodells. Migration in das Betriebsmodell C (Überführung der Plattform auf Systeme des Kunden) nur im Rahmenvertrag, nach Leistungsschein	nach Angebot
Anbindung eines zusätzlichen Fremdsystems	nach Aufwand zum Stundensatz von 249 Euro; auf Wunsch des Kunden nennt der Anbieter vorab den geschätzten Aufwand
Leistungen über den unentgeltlichen Wechsel nach dem Paragraphen zur Abwicklung nach Vertragsende hinaus, je Stunde	249
Mehraufwand wegen verletzter Mitwirkungspflichten, je Stunde	249
Vor-Ort-Kontrolle nach Anlage 4 Ziffer 5, je Stunde	249
Wechsel zwischen den Betriebsmodellen A1 und A2, je Stunde	249
Unterstützung bei Beendigung des Vertrages mit dem Rechenzentrum im Betriebsmodell A2, je Stunde	249
Kundenspezifische Feinabstimmung eines Modells ausschließlich für den Kunden, nur auf ausdrückliche Beauftragung; nicht für Kunden mit Berufsverschwiegenheit nach § 203 StGB	nach Angebot

8. Hochrisiko-Agenten nach Anlage 9

Aufschlag je Hochrisiko-Agent und Monat, zusätzlich zum Entgelt des Pakets oder zusätzlichen Agenten: [Betrag] Euro. Einmalige Einsatzprüfung und Freigabe nach Anlage 9 Ziffer 2 je Hochrisiko-Agent: [Betrag] Euro. Die Nachlässe nach Ziffer 5 gelten auch für den Aufschlag.

Anlage 3 – Verfügbarkeit und Betreuung

Diese Anlage gilt für die Betriebsmodelle A1 und A2. Im Betriebsmodell A2 gilt der Verfügbarkeitswert nur, soweit die Ursache einer Störung nicht beim vom Kunden beauftragten Rechenzentrum liegt. Im Betriebsmodell C besteht keine Verfügbarkeitszusage; dort gilt Anlage 7 Abschnitt 7.

1. Verfügbarkeit

(1) Der Anbieter gewährleistet eine Verfügbarkeit am Übergabepunkt von **99,0 %** im Monatsmittel. Im Betriebsmodell A2 gilt dieser Wert nur, soweit die Ursache einer Störung nicht in der Umgebung des Kunden oder beim von ihm beauftragten Rechenzentrum liegt.

(2) Als verfügbar gilt die Plattform, wenn die Anmeldung möglich ist und Agenten Vorgänge annehmen können. Gemessen wird durch das Überwachungssystem des Anbieters in Abständen von höchstens fünf Minuten.

(3) Nicht als Ausfallzeit gelten angekündigte Wartungsfenster, Störungen außerhalb des Verantwortungsbereichs des Anbieters, Störungen bei Vorlieferanten von Modellen, Störungen in Systemen des Kunden, Zeiten berechtigter Sperrung oder Drosselung sowie höhere Gewalt.

2. Wartungsfenster

Planbare Wartung erfolgt **sonntags 2 bis 6 Uhr** und wird mindestens **72** Stunden im Voraus angekündigt. Sie gilt nicht als Ausfallzeit.

3. Betreuung und Reaktionszeiten

Paket	Erreichbarkeit	Kanäle	Reaktionszeit
Test	Mo-Fr 8-18 Uhr	E-Mail	48 Stunden
Business	Mo-Fr 8-18 Uhr	E-Mail	24 Stunden
Pro	Mo-Fr 8-18 Uhr	E-Mail und Telefon	8 Stunden
Enterprise	Mo-Fr 8-18 Uhr	E-Mail, Telefon, fester Ansprechpartner	4 Stunden
On-Premise	Mo-Fr 8-18 Uhr	nach Anlage 7	8 Stunden

Reaktionszeit ist die Zeit bis zur ersten qualifizierten Rückmeldung innerhalb der Servicezeiten. Eine Zusage zur Dauer bis zur Behebung wird nicht gegeben.

Servicezeiten sind montags bis freitags von 8 bis 18 Uhr deutscher Zeit, ausgenommen bundeseinheitliche gesetzliche Feiertage sowie der 24. und der 31. Dezember. Reaktionszeiten laufen nur innerhalb der Servicezeiten. Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Anlage 4 Ziffer 3 und Meldungen zu Hochrisiko-Agenten nach Anlage 9 Ziffer 7 sind von den Servicezeiten unabhängig.

Störungsklassen: Eine Betriebsverhinderung liegt vor, wenn die Plattform oder ein Agent insgesamt nicht genutzt werden kann. Eine Betriebsbeeinträchtigung liegt vor, wenn eine wesentliche Funktion erheblich eingeschränkt ist, die Nutzung aber mit Einschränkungen oder über einen zumutbaren Umweg möglich bleibt. Alle übrigen Abweichungen sind sonstige Störungen. Die Reaktionszeiten der Tabelle gelten für Betriebsverhinderungen und Betriebsbeeinträchtigungen; sonstige Störungen werden im Rahmen der regulären Pflege bearbeitet.

4. Gutschriften bei Unterschreitung

Erreichte Verfügbarkeit im Monat	Gutschrift auf das Monatsentgelt
unter 99,0 % bis 98,0 %	5 %
unter 98,0 % bis 95,0 %	10 %
unter 95,0 %	20 %

Gutschriften sind innerhalb von dreißig Kalendertagen nach Ablauf des betroffenen Monats in Textform geltend zu machen und auf das Monatsentgelt begrenzt. Sie gelten als pauschalisierte Minderung. Weist der Kunde nach, dass die Gebrauchstauglichkeit in höherem Maße gemindert war, bleibt ihm die weitergehende Minderung vorbehalten; die Gutschrift wird angerechnet. Schadensersatzansprüche nach dem Paragraphen zur Haftung bleiben unberührt; Gutschriften werden auf sie angerechnet.

Anlage 4 – Vereinbarung zur Auftragsverarbeitung

1. Gegenstand, Rollen und Anwendungsbereich

(1) Der Kunde ist Verantwortlicher, der Anbieter Auftragsverarbeiter im Sinne des Art. 4 Nummern 7 und 8 DSGVO. Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung. Die vertragsgemäße Nutzung der Plattform gilt als Weisung.

(2) In den Betriebsmodellen A1 und A2 gilt diese Anlage vollumfänglich. Im Betriebsmodell A1 ist das vom Anbieter beauftragte Rechenzentrum Unterauftragsverarbeiter nach Ziffer 6. Im Betriebsmodell A2 ist das vom Kunden beauftragte Rechenzentrum Auftragsverarbeiter des Kunden; dieser schließt die erforderliche Vereinbarung selbst ab und weist sie dem Anbieter auf Verlangen nach.

(3) Im Betriebsmodell C verarbeitet der Anbieter keine Kundendaten. Diese Anlage gilt dort ausschließlich für vereinbarte Fernwartungsleistungen und ist auf den dabei anfallenden Zugriff beschränkt.

(4) Im Rahmen einer vom Kunden gesondert beauftragten kundenspezifischen Feinabstimmung (Anlage 2 Ziffer 7) bleibt der Anbieter Auftragsverarbeiter; die Beauftragung gilt als dokumentierte Weisung im Sinne des Absatzes 1. Soweit der Anbieter Daten nach Stufe 3 der Anlage 8 für die allgemeine Modellentwicklung verwendet, ist er insoweit eigener Verantwortlicher im Sinne des Art. 4 Nummer 7 DSGVO; diese Verarbeitung ist nicht Gegenstand dieser Anlage.

2. Art, Umfang und Zweck der Verarbeitung

Angabe	Inhalt
Zweck	Bearbeitung der Vorgänge, die im Datenblatt der gebuchten Agenten (Anlage 1 Ziffer 4) beschrieben sind
Art der Verarbeitung	Erheben, Speichern, Auslesen, Verwenden, Übermitteln an die vom Kunden angebundenen Systeme, Löschen
Kategorien betroffener Personen	laut Datenblatt der gebuchten Agenten (Zeile „Betroffene Personengruppen“)
Kategorien personenbezogener Daten	laut Datenblatt der gebuchten Agenten (Zeile „Verarbeitete Datenkategorien“)
Besondere Kategorien nach Art. 9 DSGVO	nur nach vorheriger Abstimmung (Anlage 6 Ziffer 2) und Angabe im Datenblatt des Agenten
Dauer	Vertragslaufzeit zuzüglich der Abruf- und Löschfrist nach dem Paragraphen zur Abwicklung nach Vertragsende (§ 26 Abs. 5)
Ort der Verarbeitung	Rechenzentrum nach Ziffer 6; ausschließlich in der Europäischen Union

3. Pflichten des Anbieters

- Verarbeitung nur auf Weisung; Hinweis, wenn eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt.
- Verpflichtung aller befassten Personen auf Vertraulichkeit.
- Umsetzung der Maßnahmen nach Art. 32 DSGVO gemäß Anlage 5.
- Unterstützung bei Betroffenenanfragen, Folgenabschätzungen und Meldepflichten in angemessenem Umfang. Für die Datenschutz-Folgenabschätzung zum Einsatz der Agenten stellt der Anbieter eine Mustervorlage bereit.

- Meldung von Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis. Die Frist läuft unabhängig von den Servicezeiten nach Anlage 3; der Anbieter hält hierfür eine auch außerhalb der Servicezeiten erreichbare Meldestelle vor und meldet so rechtzeitig, dass der Kunde seine Frist nach Art. 33 DSGVO einhalten kann.
- Löschung oder Rückgabe nach Vertragsende nach Wahl des Kunden.
- Ansprechpartner für den Datenschutz: datenschutz@codepopper.de

4. Pflichten des Kunden

Der Kunde verantwortet die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Personen und das Verzeichnis von Verarbeitungstätigkeiten. Er teilt Änderungen mit, die sich auf die Verarbeitung auswirken.

5. Kontrollrechte

Der Anbieter weist die Einhaltung vorrangig durch aktuelle Nachweise nach, insbesondere Zertifikate, Prüfberichte oder ausgefüllte Fragebögen. Vor-Ort-Kontrollen erfolgen nach Ankündigung mit angemessener Frist, während der üblichen Geschäftszeiten, höchstens einmal jährlich, ohne Störung des Betriebs und ohne Beeinträchtigung der Vertraulichkeit gegenüber anderen Kunden. Der Aufwand wird nach Anlage 2 vergütet, sofern die Kontrolle nicht aus einem vom Anbieter zu vertretenden Anlass erfolgt.

6. Unterauftragsverarbeiter

(1) Der Kunde stimmt dem Einsatz der nachfolgenden Unterauftragsverarbeiter zu. Änderungen kündigt der Anbieter mit einer Frist von dreißig Kalendertagen in Textform an und nennt dabei Unternehmen, Leistung und Verarbeitungsort. Der Kunde kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen; ist eine Fortsetzung dann nicht zumutbar, kann jede Partei mit einer Frist von einem Monat kündigen.

Unternehmen	Leistung	Sitz und Verarbeitungsort
[Rechenzentrum – nach Auswahl]	Bereitstellung und Betrieb der Server und Grafikkarten, auf denen Plattform und Modelle laufen (Hosting); kein Zugriff auf Inhalte	[Sitz – nach Auswahl]; Verarbeitungsort Finnland
[weitere]	[...]	[...]

(2) Die Modelle, mit denen die Plattform Daten des Kunden verarbeitet, betreibt der Anbieter selbst: im Betriebsmodell A1 auf von ihm beschafften Servern und Grafikkarten ausschließlich in Rechenzentren innerhalb der Europäischen Union, im Betriebsmodell A2 auf den dort vorgesehenen Systemen. Daten des Kunden werden nicht an Hersteller von Modellen übermittelt; die Hersteller der eingesetzten Modelle sind keine Unterauftragsverarbeiter. Ein von einem Dritten betriebenes Modell setzt der Anbieter nur ein, wenn dieser Dritte nach Absatz 1 als Unterauftragsverarbeiter aufgenommen ist und die Voraussetzungen der Ziffer 8 Absatz 2 vorliegen.

(3) Greift die Plattform auf Weisung des Kunden auf Anwendungen oder Dienste zu, die der Kunde selbst nutzt, insbesondere auf Kundenbeziehungs-, Buchhaltungs-, Dokumenten- oder E-Mail-Systeme, sind deren Betreiber keine Unterauftragsverarbeiter des Anbieters. Das Vertragsverhältnis mit diesen Betreibern und seine datenschutzrechtliche Ausgestaltung liegen beim Kunden; ihre Leistungen schuldet der Anbieter nicht. Setzt der Anbieter für eine solche Anbindung einen eigenen Zwischendienst eines Dritten ein, über den Daten des Kunden übertragen werden, ist dieser Unterauftragsverarbeiter nach Absatz 1.

7. Übermittlung in Drittländer

Eine Verarbeitung außerhalb der Europäischen Union durch den Anbieter oder seine Unterauftragsverarbeiter findet nicht statt. Für Anwendungen und Dienste, die der Kunde selbst anbindet, gilt Ziffer 6 Abs. 3.

8. Keine Nutzung zu Trainingszwecken im Rahmen der Auftragsverarbeitung

(1) Der Anbieter verwendet die im Auftrag verarbeiteten Daten nicht zum Trainieren, Feinabstimmen oder sonstigen Verbessern von Modellen. Ausgenommen ist die vom Kunden gesondert beauftragte Feinabstimmung von Modellen ausschließlich für den Kunden (Anlage 2 Ziffer 7) auf dessen Weisung; sie erfolgt auf den vom Anbieter betriebenen Systemen nach Ziffer 6 Absatz 2. Eine Verwendung nach Stufe 3 der Anlage 8 erfolgt außerhalb dieser Anlage.

(2) Der Anbieter verpflichtet jeden Unterauftragsverarbeiter, Daten des Kunden weder für eigene Zwecke zu verwenden noch zum Trainieren, Feinabstimmen oder sonstigen Verbessern von Modellen einzusetzen. Durchsetzbar ist diese Verpflichtung nur, wenn sie im Vertrag oder in der Vereinbarung zur Auftragsverarbeitung mit dem Unterauftragsverarbeiter enthalten ist; Richtlinien, Hinweise oder Voreinstellungen des Unterauftragsverarbeiters genügen nicht. Ist die Verpflichtung bei einem Unterauftragsverarbeiter nicht durchsetzbar, setzt der Anbieter diesen für Daten des Kunden nicht ein.

9. Löschung und Rückgabe

Nach Vertragsende stellt der Anbieter die Daten nach dem Paragraphen zur Abwicklung nach Vertragsende zum Abruf bereit, löscht sie nach Ablauf des dort bestimmten Abrufzeitraums vollständig und bestätigt die Löschung in Textform. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

Anlage 5 – Technische und organisatorische Maßnahmen

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und ordnet sie den Betriebsmodellen zu. Soweit die Zuordnung den Kunden oder ein vom Kunden beauftragtes Rechenzentrum nennt, ist die Maßnahme keine Zusage des Anbieters, sondern eine Anforderung an den Kunden im Rahmen seiner Mitwirkungspflichten; im Betriebsmodell C gilt ergänzend Anlage 7 Ziffer 9.

Verantwortung nach Betriebsmodell:

Bereich	A1	A2	C
Zutrittskontrolle	Anbieter; Rechenzentrum als Unterauftragsverarbeiter	Kunde bzw. sein Rechenzentrum	Kunde
Zugangskontrolle	Anbieter; Nutzerkonten: Kunde	Anbieter; Nutzerkonten: Kunde	Kunde
Zugriffskontrolle	Anbieter; Rollen der Nutzer: Kunde	Anbieter; Rollen der Nutzer: Kunde	Kunde
Trennungskontrolle	Anbieter	Anbieter	Kunde
Weitergabekontrolle	Anbieter	Anbieter; Netzanbindung des Rechenzentrums: Kunde	Kunde
Eingabekontrolle	Anbieter	Anbieter	Kunde
Verfügbarkeitskontrolle	Anbieter (Systeme); Datensicherung der Kundendaten: Kunde	Anbieter (Betrieb); Infrastruktur: Kunde bzw. Rechenzentrum; Datensicherung: Kunde	Kunde
Belastbarkeit und Wiederherstellbarkeit	Anbieter	Anbieter; Infrastruktur: Kunde bzw. Rechenzentrum	Kunde
Auftragskontrolle	Anbieter	Anbieter; Rechenzentrum: Kunde	entfällt, außer Fernwartung: Anbieter
Überprüfung	Anbieter	Anbieter und Kunde je für seinen Bereich	Kunde
Besonderheiten der Plattform	Anbieter	Anbieter	Anbieter in der Software; Kunde im Betrieb

Hinweis zum Entwurf: Gelb hinterlegte und mit „[VORSCHLAG – Wert prüfen]“ gekennzeichnete Angaben sind Lückenfüller. Sie beschreiben erst dann eine Zusage, wenn geprüft ist, dass die Maßnahme tatsächlich umgesetzt ist. Vor Verwendung dieser Fassung sind die Werte zu bestätigen oder zu ersetzen und die Kennzeichnung sowie dieser Hinweis zu entfernen.

Umgesetzte Maßnahmen:

Bereich	Umgesetzte Maßnahmen
Zutrittskontrolle	[VORSCHLAG – Wert prüfen] Betrieb der Systeme ausschließlich in Rechenzentren von Unterauftragsverarbeitern mit anerkannter Zertifizierung (z. B. ISO/IEC 27001); dort elektronische Zutrittskontrolle, Videoüberwachung und Protokollierung von Besuchern. Räume des Anbieters verschlossen, Schlüsselvergabe dokumentiert.
Zugangskontrolle	[VORSCHLAG – Wert prüfen] Personenbezogene Benutzerkonten; Zwei-Faktor-Anmeldung für alle administrativen Zugänge; Passwortrichtlinie; Sperre nach wiederholten Fehlversuchen; Zugang zu Servern nur über verschlüsselte Verbindungen; Sperrung von Konten ausgeschiedener Personen unverzüglich.
Zugriffskontrolle	[VORSCHLAG – Wert prüfen] Schriftliches Rollen- und Berechtigungskonzept nach dem Grundsatz der Erforderlichkeit; administrative Rechte nur für benannte Personen; Überprüfung der Berechtigungen mindestens halbjährlich; Protokollierung administrativer Zugriffe.

Bereich	Umgesetzte Maßnahmen
Trennungskontrolle	[VORSCHLAG - Wert prüfen] Logische Trennung der Daten je Kunde über getrennte Datenbereiche und Kundenkennungen; getrennte Entwicklungs-, Test- und Produktivumgebungen; keine Verwendung von Kundendaten zum Training ohne Vereinbarung nach Anlage 8.
Weitergabekontrolle	[VORSCHLAG - Wert prüfen] Verschlüsselung aller Übertragungen nach dem Stand der Technik (mindestens TLS 1.2); Verschlüsselung gespeicherter Daten (z. B. AES-256); Datenträger werden nur verschlüsselt weitergegeben und nach anerkanntem Verfahren gelöscht oder vernichtet.
Eingabekontrolle	[VORSCHLAG - Wert prüfen] Protokollierung von Eingaben, Änderungen und Löschungen mit Benutzerkennung und Zeitstempel; Aufzeichnung von Freigaben nach § 8 Abs. 3 der Nutzungsbedingungen bzw. des Rahmenvertrags; Aufbewahrung nach dem Abschnitt „Aufbewahrungsfristen der Protokolle“.
Verfügbarkeitskontrolle	[VORSCHLAG - Wert prüfen] Tägliche Sicherung der Systeme und Konfigurationen des Anbieters an einem getrennten Ort; Wiederherstellungstests mindestens jährlich; dokumentiertes Notfallkonzept. Die Sicherung der Kundendaten obliegt nach § 8 Abs. 5 dem Kunden.
Belastbarkeit und Wiederherstellbarkeit	[VORSCHLAG - Wert prüfen] Laufende Überwachung der Systeme mit automatischer Alarmierung; Einspielen von Sicherheitsaktualisierungen nach Dringlichkeit; Wiederherstellung und Störungsbearbeitung nach den Fristen der Anlage 3.
Auftragskontrolle	[VORSCHLAG - Wert prüfen] Auswahl von Unterauftragsverarbeitern erst nach Prüfung ihrer technischen und organisatorischen Maßnahmen; Verträge nach Art. 28 DSGVO; Liste nach Anlage 4; Kontrolle anhand von Zertifikaten und Prüfberichten mindestens jährlich.
Überprüfung	[VORSCHLAG - Wert prüfen] Überprüfung und Anpassung dieser Maßnahmen mindestens jährlich sowie nach wesentlichen Änderungen oder Sicherheitsvorfällen; Dokumentation der Ergebnisse.
Besonderheiten der Plattform	[VORSCHLAG - Wert prüfen] Ein- und Ausgaben der Modelle werden nur zur Leistungserbringung verarbeitet und nicht zum Training verwendet, außer im Rahmen der Anlage 8; Aufbewahrung nach dem Abschnitt „Aufbewahrungsfristen der Protokolle“; Schutz vor Eingabemanipulation durch Trennung von Systemanweisungen und Nutzereingaben, Prüfmechanismen und die Freigabepflichten nach § 8 Abs. 2; die Aufbereitungs- und Trainingsumgebung nach Anlage 8 Ziffer 4 ist vom Produktivbetrieb getrennt und hat ein eigenes Berechtigungskonzept.

Aufbewahrungsfristen der Protokolle:

- (1) Betriebsprotokolle ohne Inhalte der Ein- und Ausgaben: **[VORSCHLAG - Wert prüfen]** 12 Monate.
- (2) Freigabeprotokolle nach § 8 Abs. 3 der Nutzungsbedingungen bzw. des Rahmenvertrags: **[VORSCHLAG - Wert prüfen]** mindestens 6 Monate; längstens bis zum Ablauf der handelsrechtlichen Aufbewahrungsfrist des zugrunde liegenden Vorgangs.
- (3) Inhalte der Ein- und Ausgaben: **[VORSCHLAG - Wert prüfen]** 30 Tage. Die Frist gilt einheitlich für alle Kunden. Mit Vertragsschluss legt der Kunde sie als dokumentierte Weisung im Sinne des Art. 28 Abs. 3 lit. a DSGVO fest. Eine abweichende Frist kann nur im Rahmenvertrag im Einzelfall vereinbart werden. Einzelne Vorgänge löscht der Anbieter vor Fristablauf auf Weisung des Kunden in Textform und bestätigt die Löschung in Textform.

(4) Nach Ablauf der Frist werden die Protokolle gelöscht. Bei Vertragsende gilt vorrangig der Paragraph zur Abwicklung nach Vertragsende (Abruf und anschließende vollständige Löschung); gesetzliche Aufbewahrungspflichten bleiben unberührt. Im Betriebsmodell C legt der Kunde die Fristen in eigener Verantwortung fest (Anlage 7 Ziffer 9).

(5) Hochrisiko-Agenten nach Anlage 9: Die automatisch erzeugten Protokolle nach Art. 12 der Verordnung (EU) 2024/1689 einschließlich der zur Rekonstruktion eines Vorgangs erforderlichen Ein- und Ausgaben werden [VORSCHLAG - Wert prüfen] mindestens 6 Monate aufbewahrt (Art. 19 und Art. 26 Abs. 6 der Verordnung); die Frist nach Absatz 3 gilt insoweit nicht. Aufzeichnungen über Modell- und Konfigurationsänderungen gehören zur technischen Dokumentation und werden zehn Jahre aufbewahrt. 

Anlage 6 – Nutzungsrichtlinie und Überlassung von Rechenleistung

1. Zulässige Nutzung

Der Kunde nutzt die Plattform für eigene betriebliche Zwecke im Rahmen der Leistungsbeschreibung und stellt sicher, dass alle Nutzer diese Richtlinie kennen und einhalten.

2. Unzulässige Nutzung

- jede rechtswidrige Nutzung sowie die Verarbeitung rechtswidrig erlangter Daten,
- die Erstellung oder Verbreitung von Inhalten, die Rechte Dritter verletzen,
- die Verarbeitung besonderer Kategorien personenbezogener Daten ohne Abstimmung nach Anlage 4,
- jeder Einsatz für eine nach Artikel 5 der Verordnung (EU) 2024/1689 verbotene Praktik; eine Zustimmung hierzu ist ausgeschlossen,
- der Einsatz für Hochrisikozwecke nach Anhang III der Verordnung (EU) 2024/1689 mit einem anderen als einem hierfür freigegebenen Hochrisiko-Agenten nach Anlage 9 sowie der Einsatz eines Hochrisiko-Agenten außerhalb seiner Zweckbestimmung,
- die Nutzung für Dritte, die Weitervermietung sowie die Weitergabe von Zugängen, Rechenleistung oder Programmfassungen,
- Versuche, Sicherheits- oder Lizenzvorkehrungen, insbesondere den Aktivierungsschlüssel, zu umgehen, Systemanweisungen auszulesen oder das Verhalten der Agenten durch manipulierte Eingaben zu unterlaufen,
- das automatisierte Erzeugen von Last ohne betrieblichen Bezug, insbesondere zur Gewinnung von Trainingsdaten oder zum Nachbilden der Plattform,
- die Erzeugung von Inhalten, die Personen täuschen sollen, ohne Kenntlichmachung des maschinellen Ursprungs,
- das Treffen von Entscheidungen, die für natürliche Personen rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, ausschließlich durch einen Agenten und ohne Prüfung durch eine befugte Person,
- die Benachteiligung natürlicher Personen wegen eines in § 1 AGG oder in Art. 21 der Charta der Grundrechte der Europäischen Union genannten Merkmals,
- die Entwicklung, Herstellung oder Steuerung von Waffen, Munition oder sonstigen Rüstungsgütern sowie von Gütern mit doppeltem Verwendungszweck ohne die erforderliche Genehmigung.

3. Folgen von Verstößen

Es gelten die Regelungen des Vertrages zum vertragsgemäßen Gebrauch. Der Kunde stellt den Anbieter von Ansprüchen Dritter frei, die auf einem Verstoß gegen diese Richtlinie beruhen.

4. Angemietete Infrastruktur in den Betriebsmodellen A1 und A2

(1) Im Betriebsmodell A1 beschafft der Anbieter Rechenzentrum, Server und Grafikkarten im eigenen Namen und auf eigene Rechnung. Der Kunde erwirbt keine eigenen Ansprüche gegen das Rechenzentrum.

(1a) Der Anbieter weist dem Kunden die erfassten Rechenstunden nach dem Paragraphen zur Beschaffung von Rechenleistung offen aus. Er dokumentiert für jede dem Kunden zugeordnete Karte die Konfiguration und den Zeitraum der Zuordnung.

(2) Im Betriebsmodell A2 schließt der Kunde auf eigenen Wunsch den Vertrag mit dem Rechenzentrum im eigenen Namen. Mit der Verwaltungspauschale nach Anlage 2 abgegolten sind folgende Leistungen des Anbieters: Empfehlung einer geeigneten Ausstattung, Unterstützung bei Auswahl und Beauftragung des Rechenzentrums, Einrichtung sowie Betrieb und Überwachung der Plattform auf der vom Kunden angemieteten Infrastruktur. Diese Beschreibung ist für das Betriebsmodell A2 abschließend. Der Kunde erteilt dem Anbieter die zum Betrieb

erforderlichen Zugänge und eine Vollmacht für technische Erklärungen. Bestellungen, die zusätzliche Kosten auslösen, bedürfen der vorherigen Zustimmung des Kunden in Textform.

(3) Empfohlene Ausstattung je fünf Agenten: [Zulieferung Technik: Grafikkarte, Arbeitsspeicher, Speicherplatz, Netzanbindung, Standortanforderungen]

(4) Der Anbieter überwacht Auslastung und Kosten und weist den Kunden auf erkennbar unwirtschaftliche Konfigurationen hin. Eine Pflicht zur Kostenoptimierung besteht nur im vereinbarten Umfang.

(5) Wird Kapazität mit einer Mindestlaufzeit gebunden, teilt der Anbieter dies vor der Bindung in Textform mit. Im Betriebsmodell A2 entstehen die Bindungen unmittelbar im Verhältnis zwischen Kunde und Rechenzentrum.

5. Überlassung von Hardware in Räumen des Kunden (entfällt)

Eine Überlassung von Hardware des Anbieters in Räumen des Kunden (bisheriges Betriebsmodell B) wird nicht angeboten. Die Rechenleistung wird in den Betriebsmodellen A1 und A2 nach Ziffer 4 bereitgestellt.

Anlage 7 – Betrieb auf Systemen des Kunden (On-Premise)

Diese Anlage gilt nur, wenn die Parteien das Betriebsmodell C vereinbart haben. Sie geht den übrigen Anlagen für dieses Betriebsmodell vor; für Hochrisiko-Agenten geht Anlage 9 vor.

1. Überlassene Bestandteile

Der Anbieter überlässt dem Kunden zur Installation auf dessen Systemen:

- die Plattformsoftware in ausführbarer Form,
- die für den Betrieb erforderlichen Modelle einschließlich Modellgewichte,
- die Konfiguration der beauftragten Agenten,
- die Installations-, Betriebs- und Sicherheitsdokumentation,
- einen zeitlich befristeten Aktivierungsschlüssel.

Ein Anspruch auf Überlassung des Quellcodes besteht nicht. Eine Hinterlegung des Quellcodes bei einer neutralen Stelle kann gesondert vereinbart werden.

2. Umfang und Grenzen der Lizenz

(1) Der Kunde erhält ein einfaches, nicht ausschließliches, nicht übertragbares und nicht unterlizenzierbares Recht, die überlassenen Bestandteile für die Vertragsdauer auf den im Leistungsschein bezeichneten Systemen zu betreiben.

(2) **Zulässige Installationen: laut Leistungsschein.** Kopien dürfen ausschließlich zu Sicherungszwecken erstellt werden.

(3) Der Kunde darf die überlassenen Bestandteile nicht Dritten zugänglich machen, nicht zurückentwickeln, nicht dekompile, Modellgewichte weder extrahieren noch weitergeben und abgeleitete Modelle, insbesondere durch Feinabstimmung, nur nach Ziffer 10 erstellen. Ein Betrieb für Dritte, insbesondere als Rechenzentrums- oder Beratungsleistung, ist untersagt.

(4) Der Kunde darf die Software nicht verändern. Konfigurationen im vorgesehenen Rahmen sind zulässig und gelten nicht als Veränderung.

3. Rechte Dritter an den Modellen

(1) Die überlassenen Modelle unterliegen den Lizenzbedingungen ihrer jeweiligen Rechteinhaber. Diese sind dem Kunden vor der Überlassung zugänglich zu machen und sind für ihn verbindlich: **Qwen3.8-27B · Rechteinhaber: Alibaba Cloud (Qwen-Team) · Lizenz: Apache License 2.0 · Beschränkungen: keine Nutzungsbeschränkung; bei Weitergabe sind Lizenztext und Hinweisdateien beizufügen und Veränderungen kenntlich zu machen; keine Nutzung von Marken des Rechteinhabers. Vom Anbieter feinabgestimmte Fassungen: Rechte des Anbieters nach Ziffer 2.**

(2) Der Kunde hält die Beschränkungen dieser Lizenzen ein und stellt den Anbieter von Ansprüchen frei, die auf einem Verstoß beruhen.

(3) Der Anbieter kann eingesetzte Modelle austauschen, wenn ein Rechteinhaber seine Bedingungen ändert oder die Lizenz beendet. Er stellt in diesem Fall eine gleichwertige Programmfassung bereit.

4. Systemvoraussetzungen und Inbetriebnahme

(1) Der Kunde stellt Systeme bereit, die den Mindestanforderungen nach Anlage 1 Abschnitt 2 entsprechen, und trägt sämtliche Kosten für Hardware, Strom, Kühlung, Netz und Betrieb.

(2) Die Installation erfolgt gemeinsam. Über die Inbetriebnahme wird ein Protokoll erstellt. Mit dem Protokoll gilt die Bereitstellung als erbracht.

(3) Der Kunde benennt mindestens zwei technische Ansprechpartner mit ausreichender Berechtigung.

5. Programmfassungen und Pflege

- (1) Der Anbieter stellt während der Vertragslaufzeit neue Programmfassungen bereit, mindestens **vierteljährlich**. Sicherheitsrelevante Fassungen stellt er unverzüglich bereit.
- (2) Der Kunde spielt sicherheitsrelevante Fassungen innerhalb von **30** Kalendertagen ein. Unterlässt er dies, entfallen insoweit Mängelansprüche und die Haftung des Anbieters für hierauf beruhende Schäden.
- (3) Der Anbieter unterstützt eine überlassene Programmfassung längstens **12** Monate nach Bereitstellung der jeweils folgenden Fassung.

6. Betreuung und Fernwartung

- (1) Die Betreuung erfolgt nach Anlage 3 Ziffer 3 in der für das Betriebsmodell C ausgewiesenen Ausprägung.
- (2) Eine Fernwartung findet nur nach gesonderter Vereinbarung, auf Anforderung des Kunden und über einen von ihm freigegebenen Zugang statt. Jeder Zugriff wird protokolliert und dem Kunden auf Verlangen offengelegt. Für die dabei anfallende Verarbeitung gilt Anlage 4 im eingeschränkten Umfang.
- (3) Ohne Fernwartung ist der Kunde verpflichtet, dem Anbieter zur Störungsanalyse die erforderlichen Protokolldaten in bereinigter Form zur Verfügung zu stellen. Kann eine Störung ohne diese Mitwirkung nicht eingegrenzt werden, ruhen die Pflichten des Anbieters.

7. Keine Verfügbarkeitszusage

Der Betrieb liegt vollständig beim Kunden. Der Anbieter gibt keine Verfügbarkeitszusage ab und schuldet keine Gutschriften. Er haftet nicht für Ausfälle, Datenverluste, Sicherheitsvorfälle oder Fehlkonfigurationen in der Umgebung des Kunden.

8. Lizenzkontrolle

Der Kunde erteilt dem Anbieter einmal jährlich in Textform Auskunft über Anzahl und Standorte der Installationen sowie über die Anzahl der aktivierten Agenten. Bei konkreten Anhaltspunkten für eine Überschreitung kann der Anbieter eine Prüfung durch einen zur Verschwiegenheit verpflichteten Dritten verlangen. Die Kosten trägt der Anbieter, es sei denn, es wird eine Überschreitung von mehr als fünf Prozent festgestellt. Nachvergütet wird rückwirkend ab dem Zeitpunkt der Überschreitung.

9. Verantwortung des Kunden

Der Kunde ist im Betriebsmodell C allein verantwortlich für Betrieb, Absicherung, Zugriffsverwaltung, Protokollierung, Datensicherung und Wiederherstellung sowie für die Erfüllung aller datenschutz- und aufsichtsrechtlichen Pflichten in seiner Umgebung. Er ist datenschutzrechtlich alleiniger Verantwortlicher.

10. Verordnung über künstliche Intelligenz

- (1) Der Kunde bringt die überlassene Plattform nicht unter eigenem Namen oder eigener Marke in Verkehr, stellt sie keinem Dritten bereit und nimmt keine wesentliche Veränderung vor. Andernfalls wird er nach Art. 25 der Verordnung (EU) 2024/1689 selbst Anbieter und trägt sämtliche daraus folgenden Pflichten allein. Der Anbieter stellt die für die Betreiberpflichten erforderlichen Informationen und die technische Dokumentation bereit.
- (2) Der Kunde übermittelt dem Anbieter einmal jährlich, gemeinsam mit der Auskunft nach Ziffer 8, in Textform eine Aufstellung der tatsächlich betriebenen Agenten mit Bezeichnung, Zweckbestimmung und Einsatzbereich. Er gibt an, ob ein Agent abweichend vom Datenblatt nach Anlage 1 eingesetzt wird, und führt die Feinabstimmungen nach Absatz 4 mit dem jeweils eingesetzten Rechenaufwand auf.
- (3) Will der Kunde die Zweckbestimmung eines Agenten ändern oder einen Agenten für einen Zweck einsetzen, der nach Anhang III der Verordnung (EU) 2024/1689 als Hochrisiko einzuordnen ist, teilt er dies dem Anbieter vor der Änderung in Textform mit. Für Hochrisikozwecke gilt das Freigabeverfahren nach dem Paragraphen zur Verordnung über künstliche Intelligenz des Rahmenvertrages und nach Anlage 9.

(4) Eine Feinabstimmung oder sonstige Weiterentwicklung der überlassenen Modelle ist nur nach vorheriger Zustimmung des Anbieters in Textform zulässig. Der Kunde teilt vor Beginn Zweck, verwendete Datenarten und den voraussichtlichen Rechenaufwand mit, dokumentiert für jeden Lauf den tatsächlichen Rechenaufwand in Grafikkarten-Stunden und, soweit bestimmbar, in Gleitkommaoperationen und legt diese Dokumentation dem Anbieter auf Verlangen vor. Die Beschränkungen nach den Ziffern 2 und 3 gelten für abgeleitete Modelle entsprechend; bei Vertragsende sind sie nach Ziffer 12 zu löschen.

(5) Erreicht der Rechenaufwand einer Feinabstimmung ein Drittel des für das Training des Ausgangsmodells eingesetzten Rechenaufwands, wird der Kunde nach den Leitlinien der Kommission zu Modellen mit allgemeinem Verwendungszweck Anbieter des veränderten Modells und trägt die Pflichten nach den Artikeln 53 ff. der Verordnung allein; er unterrichtet den Anbieter hierüber unverzüglich. Der Anbieter teilt dem Kunden auf Verlangen den ihm bekannten Rechenaufwand des Ausgangsmodells mit. Unabhängig davon wird der Kunde nach Art. 25 der Verordnung Anbieter, wenn er durch eine Feinabstimmung eine wesentliche Veränderung vornimmt oder die Zweckbestimmung ändert.

(6) Für Hochrisiko-Agenten im Betriebsmodell C gilt ergänzend Anlage 9 Ziffer 9, insbesondere zur Aufbewahrung und Übermittlung der Protokolle, zur Frist für das Einspielen korrigierender Programmfassungen und zu Feinabstimmungen.

11. Ausfuhr- und Sanktionsrecht

Der Kunde hält bei Nutzung und etwaiger Verbringung der überlassenen Bestandteile die geltenden Ausfuhr-, Einfuhr- und Sanktionsvorschriften ein und setzt sie nicht in **Liste ausgeschlossener Länder und Empfänger** ein.

12. Beendigung

Mit Vertragsende erlischt das Nutzungsrecht. Der Kunde stellt den Betrieb ein, deinstalliert die Software vollständig, löscht alle Kopien einschließlich der Modellgewichte und der nach Ziffer 10 abgeleiteten Modelle und weist dies innerhalb von vierzehn Kalendertagen in Textform nach. Der Aktivierungsschlüssel verliert seine Gültigkeit. Der Anbieter ist berechtigt, die technische Funktionsfähigkeit nach Ablauf der Laufzeit zu beenden.

Anlage 8 – Datenpartnerschaft

Gesonderte Vereinbarung über die Verwendung von Daten zur Entwicklung von Modellen

1. Gegenstand und Freiwilligkeit

- (1) Der Anbieter entwickelt eigene Modelle und passt Modelle an. Hierfür benötigt er Beispieldaten aus dem praktischen Betrieb.
- (2) Der Kunde kann dem Anbieter freiwillig gestatten, Daten aus seinem Betrieb hierfür zu verwenden. Die Teilnahme ist in Stufen wählbar, jederzeit für die Zukunft widerruflich und wird nach Anlage 2 Ziffer 6 vergütet.
- (3) Die Teilnahme ist keine Voraussetzung für den Vertragsschluss, für die Nutzung der Plattform oder für einen bestimmten Leistungsumfang. Ein Kunde, der nicht teilnimmt, erhält dieselbe Leistung.

2. Stufen der Teilnahme

Stufe	Was verwendet wird	Zweck und Rolle
Stufe 0 – keine Nutzung	nichts über den Betrieb hinaus	Regelfall, gilt ohne gesonderte Zustimmung
Stufe 1 – Betriebskennzahlen	aggregierte, nicht personenbezogene und nicht auf den Kunden rückführbare Kennzahlen zu Auslastung, Laufzeiten, Fehlern und Abbruchgründen	Betrieb, Abrechnung, Störungsbeseitigung, Verbesserung der Plattform. Bereits im Hauptvertrag geregelt, keine gesonderte Zustimmung erforderlich.
Stufe 3 – allgemeine Modellentwicklung	anonymisierte oder synthetisch abgeleitete Inhalte nach dem Verfahren der Ziffer 4	Entwicklung und Verbesserung der Modelle des Anbieters für alle Kunden. Der Anbieter ist insoweit eigener Verantwortlicher.

3. Ausgeschlossene Kunden und ausgeschlossene Daten

(1) **Von der Teilnahme an der Stufe 3 ausgeschlossen** sind Kunden, die einer Berufsverschwiegenheit nach § 203 StGB unterliegen, insbesondere Rechtsanwältinnen und Rechtsanwälte, Steuerberatung, Wirtschaftsprüfung, Notariat, Ärztinnen und Ärzte, Psychotherapie, Apotheken und Angehörige weiterer dort genannter Berufe. Eine Zustimmung dieser Kunden ist unwirksam.

(2) Ausgeschlossen sind unabhängig von der Stufe:

- besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten über strafrechtliche Verurteilungen und Straftaten,
- Daten von Kindern und Jugendlichen,
- Daten, die einer gesetzlichen Geheimhaltungspflicht oder einer Verschwiegenheitsvereinbarung mit einem Dritten unterliegen,
- Beschäftigtendaten, soweit nicht eine Betriebsvereinbarung oder eine andere tragfähige Grundlage vorliegt,
- Geschäftsgeheimnisse Dritter sowie vom Kunden als vertraulich gekennzeichnete Inhalte,
- Inhalte, an denen erkennbar Urheberrechte Dritter bestehen, **soweit deren Nutzung nicht zulässig ist.**

(3) Der Kunde kann einzelne Agenten, Abteilungen oder Vorgangstypen von der Teilnahme ausnehmen. Der Anbieter stellt hierfür eine Einstellmöglichkeit bereit.

4. Aufbereitung vor der Verwendung

Der Anbieter verwendet Daten nach Stufe 3 erst nach folgendem Verfahren:

- automatisierte Erkennung und Entfernung direkter Identifikatoren, insbesondere Namen, Anschriften, Kontaktdaten, Konto- und Ausweisnummern,
- Entfernung oder Ersetzung indirekter Identifikatoren, soweit eine Wiedererkennung möglich bliebe,
- Entfernung von Kennzeichen, die auf den Kunden schließen lassen, insbesondere Firmierungen, Logos und Belegnummernkreise,
- stichprobenartige Prüfung durch geschulte Personen im Umfang von mindestens 0,5 % der Datensätze je Aufbereitungslauf; ergibt die Prüfung Hinweise auf nicht entfernte Identifikatoren, wird die Stichprobe auf bis zu 5 % erweitert und die Aufbereitung vor der Verwendung nachgebessert,
- Speicherung der aufbereiteten Daten getrennt vom Produktivbetrieb und mit eigenem Berechtigungskonzept,
- Löschung der unaufbereiteten Ausgangsdaten spätestens 30 Kalendertage nach der Aufbereitung.

Der Anbieter unterlässt jeden Versuch einer Wiederherstellung des Personenbezugs und verpflichtet die beteiligten Personen entsprechend.

5. Pflichten des Anbieters

- Er führt ein Verzeichnis der verwendeten Datenbestände und dokumentiert Herkunft, Aufbereitung und Verwendungszweck.
- Er prüft vor jeder Veröffentlichung eines Modells, ob dieses Inhalte aus Kundendaten wörtlich oder nahezu wörtlich wiedergibt, und ergreift wirksame Gegenmaßnahmen.
- Er stellt dem Kunden auf Verlangen einmal jährlich eine Zusammenfassung darüber zur Verfügung, in welchem Umfang dessen Daten verwendet wurden.
- Er unterhält eine eigene Datenschutzhinweise für die Verarbeitung nach Stufe 3 und benennt darin die Rechtsgrundlage.
- Er gibt aufbereitete Daten nicht an Dritte weiter und verwendet sie nicht für Zwecke außerhalb der Modellentwicklung.

6. Zusicherungen des Kunden

Der Kunde sichert für die von ihm freigegebenen Datenbestände zu, dass

- er zur Erteilung der Erlaubnis berechtigt ist und keine Rechte Dritter entgegenstehen,
- er die betroffenen Personen im gesetzlich gebotenen Umfang über die Verwendung unterrichtet hat,
- für die Verarbeitung eine tragfähige Rechtsgrundlage besteht und er diese dokumentiert hat,
- erforderliche Beteiligungsrechte, insbesondere solche des Betriebsrats, gewahrt sind,
- die nach Ziffer 3 ausgeschlossenen Daten nicht enthalten sind.

Der Kunde stellt den Anbieter von Ansprüchen Dritter sowie von den angemessenen Kosten der Rechtsverteidigung, auch in behördlichen Verfahren, frei, soweit diese auf einer schuldhaften Verletzung dieser Zusicherungen beruhen. Der Anbieter unterrichtet ihn unverzüglich über die Inanspruchnahme.

7. Verordnung über künstliche Intelligenz und Urheberrecht

(1) Der Anbieter erfüllt die für die Entwicklung von Modellen geltenden Pflichten, insbesondere zur Datenqualität und zur Dokumentation der verwendeten Datenquellen, in eigener Verantwortung.

(2) Soweit er ein Modell mit allgemeinem Verwendungszweck entwickelt, erfüllt er die hierfür geltenden Transparenz- und Dokumentationspflichten und veröffentlicht die vorgeschriebene Zusammenfassung über die verwendeten Inhalte.

(3) Der Anbieter beachtet Vorbehalte der Rechteinhaber gegen die Nutzung zum Text- und Data-Mining, soweit ihm solche Inhalte über den Kunden zugehen.

(4) Verwendet der Anbieter Daten, die aus Hochrisiko-Agenten nach Anlage 9 stammen, oder Daten für das Training, die Validierung oder das Testen von Modellen, die in Hochrisiko-Agenten eingesetzt werden, erfüllt er die Anforderungen des Art. 10 der Verordnung (EU) 2024/1689 an Daten und Daten-Governance, insbesondere zur Herkunft, Qualität, Repräsentativität und Prüfung auf Verzerrungen, und dokumentiert sie in der technischen Dokumentation. Die Ausschlüsse nach Ziffer 3 bleiben unberührt.

8. Widerruf und dessen Grenzen

(1) Der Kunde kann seine Zustimmung jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft in Textform oder in der Verwaltungsoberfläche widerrufen. Der Anbieter setzt den Widerruf unverzüglich, spätestens innerhalb von vierzehn Kalendertagen um.

(2) Mit dem Widerruf endet die weitere Verwendung. Der Anbieter löscht die noch nicht in ein Modell eingeflossenen aufbereiteten Datenbestände des Kunden.

(3) Der Kunde nimmt zur Kenntnis und erkennt an, dass bereits abgeschlossene Trainingsläufe und die daraus hervorgegangenen Modelle technisch nicht rückgängig gemacht werden können. Ein Anspruch auf Entfernung bereits erfolgter Lernbeiträge aus einem bestehenden Modell besteht nicht. Der Anbieter wird jedoch bei der nächsten grundlegenden Neuentwicklung eines Modells die Daten des widerrufenden Kunden nicht erneut verwenden.

(4) Mit dem Widerruf entfällt der Nachlass nach Anlage 2 Ziffer 6 ab dem folgenden Abrechnungszeitraum.

(5) Absatz 3 lässt Rechte betroffener Personen nach der Datenschutz-Grundverordnung unberührt. Macht eine betroffene Person Rechte geltend, stimmen sich die Parteien unverzüglich über das weitere Vorgehen ab.

9. Betriebsmodell C

Im Betriebsmodell C hat der Anbieter keinen Zugriff auf Daten des Kunden. Eine Teilnahme ist nur möglich, wenn der Kunde ausgewählte Datenbestände aktiv und ausdrücklich bereitstellt. Umfang, Format und Übergabeweg werden gesondert in Textform vereinbart. Ein automatisierter Abfluss aus Systemen des Kunden findet nicht statt.

10. Zustimmungserklärung

Der Kunde erklärt, diese Anlage gelesen und verstanden zu haben, und wählt die folgende Stufe. Ohne Auswahl gilt Stufe 0.

Auswahl	Stufe	Nachlass nach Anlage 2 Ziffer 6
☐	Stufe 0 – keine Nutzung meiner Daten zur Modellentwicklung	kein Nachlass
☐	Stufe 3 – Verwendung zur allgemeinen Modellentwicklung des Anbieters	15 %

Der Kunde bestätigt zusätzlich ausdrücklich:

- Er unterliegt keiner Berufsverschwiegenheit nach § 203 StGB.
- Er hat die Zusicherungen nach Ziffer 6 geprüft und kann sie abgeben.
- Er hat zur Kenntnis genommen, dass bereits abgeschlossene Trainingsläufe nach Ziffer 8 Absatz 3 nicht rückgängig gemacht werden können.

Ort, Datum

Ort, Datum

Anbieter

Kunde

Anlage 9 – Hochrisiko-Agenten

Diese Anlage gilt nur, soweit ein Hochrisiko-Agent gebucht ist – im Online-Abschluss über die Bestellung, im Rahmenvertrag über den Leistungsschein. Sie geht für Hochrisiko-Agenten den Anlagen 1, 2, 3 und 5 bis 8 vor; Anlage 4 bleibt unberührt. Begriffe und Artikel beziehen sich auf die Verordnung (EU) 2024/1689 (Verordnung).

1. Gegenstand und Anwendungsbereich

(1) Hochrisiko-Agenten sind Agenten, die der Anbieter für einen Zweck nach Anhang III der Verordnung als Hochrisiko-KI-System in Verkehr bringt. Der Anbieter ist für sie Anbieter im Sinne des Art. 3 Nr. 3 der Verordnung, der Kunde Betreiber im Sinne des Art. 3 Nr. 4.

(2) Hochrisiko-Agenten werden ausschließlich in folgenden Bereichen des Anhangs III angeboten:

- Nr. 3 – allgemeine und berufliche Bildung, insbesondere Zugang und Zulassung, Bewertung von Lernergebnissen, Bewertung des angemessenen Bildungsniveaus und Überwachung von Prüfungen,
- Nr. 4 – Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit, insbesondere Einstellung und Auswahl, Entscheidungen über Beförderung und Beendigung, Aufgabenzuweisung sowie Beobachtung und Bewertung von Leistung und Verhalten,
- Nr. 5 Buchst. a – Beurteilung von Ansprüchen natürlicher Personen auf grundlegende öffentliche Unterstützungsleistungen und Dienste durch Behörden oder in deren Auftrag,
- Nr. 5 Buchst. b – Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen, mit Ausnahme der Aufdeckung von Finanzbetrug,
- Nr. 5 Buchst. c – Risikobewertung und Preisbildung in Bezug auf natürliche Personen in der Lebens- und Krankenversicherung.

Andere Bereiche des Anhangs III werden nicht angeboten; ein Einsatz der Plattform für diese Bereiche ist nach § 19 Abs. 3 der Nutzungsbedingungen bzw. des Rahmenvertrages nicht zulässig.

(3) Zweckbestimmung, Leistungsmerkmale und Grenzen jedes Hochrisiko-Agenten ergeben sich aus seiner Betriebsanleitung nach Ziffer 3 und seinem Datenblatt nach Anlage 1 Ziffer 4. Ein Einsatz außerhalb der Zweckbestimmung ist nicht vertragsgemäß.

(4) Hochrisiko-Agenten können in den Paketen Business, Pro und Enterprise sowie im Betriebsmodell C gebucht werden, nicht im Paket Test. Im Betriebsmodell C gilt ergänzend Ziffer 9.

2. Buchung, Einsatzprüfung und Freigabe

(1) Vor der Buchung macht der Kunde die Angaben nach § 19 Abs. 12 für jeden gewünschten Hochrisiko-Agenten vollständig, insbesondere zum Anhang-III-Bereich, zum konkreten Einsatzzweck, zu den betroffenen Personengruppen, zur vorgesehenen menschlichen Aufsicht und dazu, ob er Behörde, öffentliche Stelle oder private Einrichtung ist, die öffentliche Dienste erbringt.

(2) Der Anbieter prüft, ob der angegebene Einsatzzweck innerhalb der Zweckbestimmung liegt. Der Hochrisiko-Agent wird erst nach Freigabe durch die Geschäftsführung des Anbieters nach § 19 Abs. 4 freigeschaltet. Der Anbieter kann die Freigabe verweigern, wenn der Einsatzzweck außerhalb der Zweckbestimmung liegt oder die Angaben unvollständig sind; bis zur Freischaltung wird für den Hochrisiko-Agenten kein Entgelt geschuldet.

(3) Mit der Freischaltung teilt der Anbieter dem Kunden in Textform mit: die Bezeichnung und Version des Hochrisiko-Agenten, die Fassung der Betriebsanleitung, die Fundstelle der EU-Konformitätserklärung und die Registriernummer in der EU-Datenbank.

3. Betriebsanleitung

(1) Für jeden Hochrisiko-Agenten stellt der Anbieter eine Betriebsanleitung nach Art. 13 der Verordnung in deutscher Sprache bereit. Setzt der Kunde den Agenten in weiteren Mitgliedstaaten ein, gibt er dies bei der Buchung an; der Anbieter stellt die erforderlichen Sprachfassungen bereit.

(2) Die Betriebsanleitung ist in der bei Freischaltung gültigen Fassung Bestandteil dieses Vertrages. Aktualisierte Fassungen stellt der Anbieter in der Verwaltungsoberfläche bereit und weist auf wesentliche Änderungen hin; der Kunde bestätigt die Kenntnisnahme in der Verwaltungsoberfläche.

(3) Die Betriebsanleitung enthält mindestens die Angaben nach Art. 13 Abs. 3 der Verordnung, insbesondere Anbieter und Kontaktdaten, Zweckbestimmung und ausgeschlossene Verwendungen, Genauigkeit, Robustheit und Cybersicherheit einschließlich der Leistung je betroffener Personengruppe, bekannte Grenzen und vorhersehbare Fehlanwendungen, Anforderungen an die Eingabedaten, Hilfen zur Interpretation der Ergebnisse, die Maßnahmen zur menschlichen Aufsicht, vorab festgelegte Änderungen, Wartung und Aktualisierung sowie die Mechanismen zur Erfassung, Aufbewahrung und Auswertung der Protokolle.

4. Pflichten des Anbieters

(1) Der Anbieter erfüllt die Pflichten eines Anbieters von Hochrisiko-KI-Systemen nach Art. 16 der Verordnung in eigener Verantwortung, insbesondere:

- Erfüllung der Anforderungen der Artikel 8 bis 15 und Betrieb eines Qualitätsmanagementsystems nach Art. 17,
- technische Dokumentation nach Art. 11 und Anhang IV sowie deren Aufbewahrung für zehn Jahre nach Art. 18,
- Aufbewahrung der automatisch erzeugten Protokolle, soweit sie seiner Kontrolle unterliegen, für mindestens sechs Monate nach Art. 19,
- Konformitätsbewertung nach Art. 43, EU-Konformitätserklärung nach Art. 47, CE-Kennzeichnung nach Art. 48 und Registrierung nach Art. 49,
- Korrekturmaßnahmen und Informationspflichten nach Art. 20 sowie Zusammenarbeit mit den zuständigen Behörden nach Art. 21,
- Beobachtung nach dem Inverkehrbringen nach Art. 72 und Meldung schwerwiegender Vorfälle nach Art. 73.

(2) Der Anbieter stellt dem Kunden in der Verwaltungsoberfläche zur Verfügung: die Informationen für die Datenschutz-Folgenabschätzung (Art. 26 Abs. 9 der Verordnung) und für die Grundrechte-Folgenabschätzung (Art. 27), Muster für die Information der Beschäftigten und ihrer Vertretung (Art. 26 Abs. 7) und der betroffenen Personen (Art. 26 Abs. 11), Informationen zur Erläuterung von Einzelentscheidungen (Art. 86), Schulungsunterlagen für die aufsichtführenden Personen sowie eine Exportfunktion für die Protokolle (Art. 26 Abs. 6).

(3) Der Anbieter unterrichtet den Kunden unverzüglich in Textform über Korrekturmaßnahmen, Rücknahmen oder Rückrufe nach Art. 20 der Verordnung sowie über Änderungen, die Zweckbestimmung, Leistungsmerkmale oder Grenzen eines Hochrisiko-Agenten betreffen.

5. Pflichten des Kunden als Betreiber

(1) Der Kunde erfüllt die Pflichten eines Betreibers nach den Artikeln 26, 27 und 86 der Verordnung in eigener Verantwortung. Insbesondere

- verwendet er den Hochrisiko-Agenten nur für den freigegebenen Einsatzzweck und gemäß der Betriebsanleitung und trifft hierfür geeignete technische und organisatorische Maßnahmen (Art. 26 Abs. 1),
- überträgt er die menschliche Aufsicht Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, lässt sie an der Schulung nach Ziffer 4 Abs. 2 teilnehmen und setzt die in der Betriebsanleitung beschriebenen Aufsichtsmaßnahmen um (Art. 26 Abs. 2, Art. 4); § 8 bleibt unberührt,
- stellt er sicher, dass die Eingabedaten, soweit sie seiner Kontrolle unterliegen, im Hinblick auf den Einsatzzweck relevant und ausreichend repräsentativ sind (Art. 26 Abs. 4),
- überwacht er den Betrieb anhand der Betriebsanleitung und unterrichtet den Anbieter über Auffälligkeiten; hat er Grund zu der Annahme, dass die Verwendung ein Risiko im Sinne des Art. 79 Abs. 1

der Verordnung birgt, unterrichtet er unverzüglich den Anbieter und die zuständige Marktüberwachungsbehörde und setzt die Verwendung aus (Art. 26 Abs. 5),

- bewahrt er die Protokolle, soweit sie seiner Kontrolle unterliegen, mindestens sechs Monate auf (Art. 26 Abs. 6),
- unterrichtet er als Arbeitgeber vor der Inbetriebnahme am Arbeitsplatz die Arbeitnehmervertretung und die betroffenen Beschäftigten und wahrt die Beteiligungsrechte des Betriebs- oder Personalrats (Art. 26 Abs. 7),
- registriert er als Behörde oder Einrichtung der Union die Verwendung vor der Inbetriebnahme in der EU-Datenbank und verwendet keinen dort nicht registrierten Hochrisiko-Agenten (Art. 26 Abs. 8, Art. 49 Abs. 3),
- führt er die Datenschutz-Folgenabschätzung durch, soweit erforderlich, und nutzt dafür die Informationen des Anbieters (Art. 26 Abs. 9),
- unterrichtet er natürliche Personen, über die der Hochrisiko-Agent Entscheidungen trifft oder bei solchen Entscheidungen unterstützt, über dessen Einsatz (Art. 26 Abs. 11) und beantwortet Verlangen auf Erläuterung nach Art. 86,
- führt er vor der ersten Verwendung eine Grundrechte-Folgenabschätzung durch und teilt deren Ergebnis der Marktüberwachungsbehörde mit, wenn er Behörde, öffentliche Stelle oder private Einrichtung ist, die öffentliche Dienste erbringt, oder einen Hochrisiko-Agenten nach Anhang III Nr. 5 Buchst. b oder c einsetzt (Art. 27),
- arbeitet er mit den zuständigen Behörden zusammen (Art. 26 Abs. 12).

(2) Der Kunde nimmt an einem Hochrisiko-Agenten keine wesentliche Veränderung vor und ändert dessen Zweckbestimmung nicht. Andernfalls wird er nach Art. 25 der Verordnung selbst Anbieter und trägt die daraus folgenden Pflichten allein; § 19 Abs. 7 gilt entsprechend.

6. Beobachtung nach dem Inverkehrbringen und Protokolle

(1) Der Anbieter beobachtet die Hochrisiko-Agenten nach Art. 72 der Verordnung anhand der automatisch erzeugten Protokolle und daraus abgeleiteter Kennzahlen, insbesondere zu Leistung, Fehlern, Übersteuerungen durch Menschen, Veränderungen im Zeitverlauf und Ergebnissen je betroffener Personengruppe. § 16 Abs. 4 Satz 2 steht dem nicht entgegen; die Auswertung dient ausschließlich der Erfüllung der Pflichten nach der Verordnung und der Sicherheit der Hochrisiko-Agenten.

(2) Die Auswertung erfolgt, soweit möglich, mit pseudonymisierten oder aggregierten Daten. Mit der Buchung eines Hochrisiko-Agenten weist der Kunde den Anbieter im Sinne der Anlage 4 Ziffer 1 an, die Protokolle für diese Zwecke zu verarbeiten und nach Anlage 5 Abschnitt „Aufbewahrungsfristen der Protokolle“ Absatz 5 aufzubewahren.

(3) Der Kunde wirkt an der Beobachtung mit. Er beantwortet Rückfragen des Anbieters zu Auffälligkeiten innerhalb angemessener Frist, stellt, soweit vorhanden und rechtlich zulässig, Rückmeldungen zur Richtigkeit von Ergebnissen bereit und leitet Beschwerden betroffener Personen nach § 19 Abs. 9 weiter.

(4) Der Anbieter stellt dem Kunden vierteljährlich einen Bericht über die Kennzahlen seiner Hochrisiko-Agenten in der Verwaltungsoberfläche bereit.

7. Schwerwiegende Vorfälle und Risiken

(1) Der Kunde meldet dem Anbieter schwerwiegende Vorfälle im Sinne des Art. 3 Nr. 49 der Verordnung sowie Umstände, die ein Risiko im Sinne des Art. 79 Abs. 1 begründen können, unverzüglich, spätestens innerhalb von **24 Stunden** nach Kenntnis, über die Meldestelle nach Anlage 4 Ziffer 2. Seine eigenen Pflichten gegenüber der Marktüberwachungsbehörde nach Art. 26 Abs. 5 bleiben unberührt. 

(2) Der Anbieter bewertet die Meldung, meldet schwerwiegende Vorfälle nach Art. 73 der Verordnung an die zuständige Marktüberwachungsbehörde und unterrichtet den Kunden über das Ergebnis. Die Parteien sichern die für die Untersuchung erforderlichen Protokolle und Unterlagen und nehmen vor der Unterrichtung der Behörde

keine Veränderung am Hochrisiko-Agenten vor, die die spätere Bewertung der Ursachen beeinträchtigen könnte (Art. 73 Abs. 6).

(3) Meldungen zu Hochrisiko-Agenten bearbeitet der Anbieter unabhängig von den Servicezeiten nach Anlage 3; die erste qualifizierte Rückmeldung erfolgt innerhalb von **24 Stunden**.

8. Korrekturmaßnahmen, Aussetzung und Abschaltung

(1) Hat der Anbieter Grund zu der Annahme, dass ein Hochrisiko-Agent nicht der Verordnung entspricht oder ein Risiko birgt, darf er ihn anpassen, aussetzen, zurücknehmen oder zurückrufen (Art. 20 der Verordnung). Er unterrichtet den Kunden unverzüglich; der Kunde setzt die mitgeteilten Maßnahmen in seinem Bereich um.

(2) Für die Dauer einer Aussetzung, die der Kunde nicht zu vertreten hat, entfällt das Entgelt für den betroffenen Hochrisiko-Agenten. Mängelrechte und die Regelungen zur Haftung bleiben unberührt.

(3) Setzt der Kunde einen Hochrisiko-Agenten außerhalb des freigegebenen Einsatzzwecks ein, gilt § 16 Abs. 4.

9. Hochrisiko-Agenten im Betriebsmodell C

(1) Hochrisiko-Agenten im Betriebsmodell C setzen eine Vereinbarung im Leistungsschein voraus. Anlage 7 gilt ergänzend; bei Widersprüchen geht diese Ziffer vor.

(2) Der Kunde bewahrt die automatisch erzeugten Protokolle mindestens sechs Monate auf und übermittelt dem Anbieter **monatlich** die für die Beobachtung nach Ziffer 6 erforderlichen Kennzahlen und Protokollauszüge in dem vom Anbieter vorgegebenen, bereinigten Format; bei Vorfällen nach Ziffer 7 unverzüglich.

(3) Korrigierende und sicherheitsrelevante Programmfassungen für Hochrisiko-Agenten spielt der Kunde abweichend von Anlage 7 Ziffer 5 Abs. 2 innerhalb von **10 Kalendertagen** ein und bestätigt die Einspielung in Textform. Maßnahmen nach Ziffer 8 setzt er innerhalb der vom Anbieter gesetzten Frist um und weist dies nach.

(4) Der Kunde stellt dem Anbieter die Informationen bereit, die dieser für die Konformitätsbewertung, die Beantwortung von Behördenanfragen und die Untersuchung von Vorfällen benötigt.

(5) Eine Feinabstimmung oder sonstige Veränderung eines Hochrisiko-Agenten durch den Kunden bedarf der vorherigen Zustimmung des Anbieters in Textform. Sie gilt als wesentliche Veränderung im Sinne des Art. 25 der Verordnung, soweit sie nicht als vorab festgelegte Änderung in der technischen Dokumentation beschrieben ist.

10. Anbindungen

(1) Der Kunde kann an Hochrisiko-Agenten Anwendungen und Dienste Dritter nach § 17 Abs. 8 anbinden; der Anbieter sperrt oder überwacht solche Anbindungen nicht. Die Betriebsanleitung nennt, welche Anbindungen Teil der Konformitätsbewertung und damit der bestimmungsgemäßen Verwendung sind.

(2) Bindet der Kunde weitere Anwendungen oder Dienste an oder verändert er die Konfiguration über den in der Betriebsanleitung vorgesehenen Rahmen hinaus, trägt er hierfür die Verantwortung. Führt dies zu einer wesentlichen Veränderung oder einer Änderung der Zweckbestimmung, gilt Ziffer 5 Abs. 2.

11. Datenpartnerschaft

Daten aus Hochrisiko-Agenten können nach Anlage 8 in die Datenpartnerschaft einbezogen werden. Die Ausschlüsse nach Anlage 8 Ziffer 3 gelten unverändert; für die Verwendung gilt Anlage 8 Ziffer 7 Abs. 4.

12. Vergütung und Aufbewahrung

(1) Die Vergütung für Hochrisiko-Agenten ergibt sich aus Anlage 2 Ziffer 8.

(2) Die technische Dokumentation und die EU-Konformitätserklärung bewahrt der Anbieter nach Art. 18 der Verordnung zehn Jahre auf; die Protokolle nach Ziffer 6 und Anlage 5 werden nach Ablauf der dort genannten Frist gelöscht. Gesetzliche Aufbewahrungspflichten gehen der Löschung nach dem Paragraphen zur Abwicklung nach Vertragsende vor.