NOCIP

Keine Cloud-Inferenz mit personenbezogenen Daten

Prüfcheckliste

Version 1.0 · 29.10.2026 · Entwurf – noch nicht freigegeben

Diese Checkliste ist für die Prüfer der be next GmbH bestimmt und wird veröffentlicht, damit Antragsteller wissen, was geprüft wird. Jede Prüfung folgt ihr vollständig; Abweichungen werden im Prüfbericht begründet. Testdaten und Prüfwerte werden nicht veröffentlicht.

1 Prüfumgebung

- Prüfumgebung: Das Produkt läuft auf einem Prüfrechner von NOCIP oder als Testzugang. Der gesamte Datenverkehr läuft über einen abfangenden Proxy (z. B. mitmproxy) mit Paketmitschnitt (alle Protokolle, nicht nur HTTP) und DNS-Protokoll.
- TLS: Das Prüfzertifikat wird installiert. Verhindert Zertifikats-Pinning die Einsicht, stellt der Anbieter eine Testversion ohne Pinning oder ein Protokoll der ausgehenden Daten bereit; sonst gelten die betroffenen Kriterien als nicht nachgewiesen.
- Prüfwerte: Für jede Prüfung werden neue, eindeutige Prüfwerte erzeugt, damit Treffer eindeutig zugeordnet werden können.
- Testkorpus: Verwendet wird die aktuelle Version des NOCIP-Testkorpus (Deutsch und Englisch); die Version steht im Prüfbericht.
- Aufbewahrung: Mitschnitte, Protokolle und Bildschirmfotos werden 3 Jahre aufbewahrt und nicht weitergegeben.

Vorbereitung

☐ Selbstauskunft vollständig, Nachweise vorhanden

☐ Testinstallation bzw. Testzugang eingerichtet

☐ Prüf-Proxy, Paketmitschnitt und DNS-Protokoll laufen; Prüfzertifikat installiert

☐ Prüfwert-Satz für diese Prüfung erzeugt (Nr. _____)

☐ Testkorpus-Version notiert (_____)

2 Prüfung je Kriterium

Alle Stufen

C-01 Offenlegung

Anforderung	Produkt und Website des Anbieters nennen die NOCIP-Stufe und sagen, wo die KI-Verarbeitung stattfindet. Die Angabe ist für Nutzer vor der ersten Verwendung auffindbar (z. B. Produktseite, Einstellungen, Dokumentation).
Schritte	☐ 1. Angaben auf der Website und im Produkt aufrufen. ☐ 2. Angaben mit der im Audit festgestellten Architektur vergleichen.

Bestanden, wenn	Angaben vorhanden, zutreffend und passend zur Stufe.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

C-02 Modellverzeichnis

Anforderung	Die Dokumentation nennt jedes Modell, das für KI-Funktionen des Produkts eingesetzt wird: Name, Version, Lizenz, Herkunft und Ort der Ausführung (Kunde, Anbieter oder Dritt-KI mit Land).
Schritte	☐ 1. Modellverzeichnis mit installierten Modelldateien, Konfiguration und beobachtetem Datenverkehr vergleichen.
Bestanden, wenn	Verzeichnis vollständig und stimmig.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

C-03 Kein Training mit Kundendaten

Anforderung	Inhalte des Kunden werden weder vom Anbieter noch von Dritten zum Training oder Nachtraining von Modellen verwendet, außer der Kunde willigt ausdrücklich ein. Die Einwilligung ist standardmäßig aus. Nachtraining ausschließlich auf den Systemen des Kunden ist erlaubt.
Schritte	☐ 1. Vertragsbedingungen prüfen. ☐ 2. Standardeinstellungen im Produkt prüfen.
Bestanden, wenn	Kein Training ohne ausdrückliche Einwilligung; Einwilligung standardmäßig aus.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

C-04 Keine Inhalte in Telemetrie und Protokollen

Anforderung	Telemetrie, Nutzungsstatistiken, Absturzberichte und entfernte Protokolle enthalten keine Dokumentinhalte, Eingaben, KI-Ergebnisse oder personenbezogenen Daten aus verarbeiteten Inhalten.
Schritte	☐ 1. Testdokumente mit Prüfwerten verarbeiten. ☐ 2. Gesamten ausgehenden Datenverkehr mitschneiden, einschließlich Absturzberichten (Absturz möglichst auslösen). ☐ 3. Mitschnitt nach Prüfwerten durchsuchen.
Bestanden, wenn	Kein Prüfwert außerhalb der für die Stufe zulässigen Übermittlungen.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	

Bemerkung	

C-05 Änderungsmeldung

Anforderung	Der Anbieter meldet Änderungen der KI-Architektur (neues Modell oder neuer Modellanbieter, neuer Verarbeitungsort, neue externe Verbindung, geänderte Weiche oder Pseudonymisierung) innerhalb von 30 Tagen an NOCIP. Eine Änderung, die zu einer niedrigeren Stufe führt, wird vor ihrer Einführung gemeldet.
Schritte	☐ 1. Label-Vereinbarung prüfen. ☐ 2. Bei Stichproben und Verlängerung: Architektur mit dem letzten Prüfbericht vergleichen.
Bestanden, wenn	Vereinbarung unterzeichnet; keine ungemeldeten Änderungen.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

C-06 Verbindungsliste

Anforderung	Der Anbieter nennt jede ausgehende Netzwerkverbindung des Produkts (Ziel, Zweck, übertragene Daten). Bei der Verarbeitung der Testdokumente entstehen keine Verbindungen außerhalb dieser Liste.
Schritte	☐ 1. Produkt hinter dem Prüf-Proxy und mit Paketmitschnitt betreiben. ☐ 2. Testkorpus verarbeiten. ☐ 3. Beobachtete Verbindungen und DNS-Anfragen mit der Liste vergleichen.
Bestanden, wenn	Keine Verbindung, die nicht auf der Liste steht.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

C-07 Auftragsverarbeitung

Anforderung	Verarbeitet der Anbieter Daten des Kunden (z. B. SaaS, Fernwartung), bietet er einen Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO an, der alle Unterauftragsverarbeiter mit Zugang zu KI-Eingaben oder -Ergebnissen nennt. Gilt nicht, wenn der Anbieter keine Kundendaten erhält.
Schritte	☐ 1. Vertrag und Liste prüfen. ☐ 2. Liste mit Modellverzeichnis und Verbindungsliste vergleichen.
Bestanden, wenn	Vertrag vorhanden; Liste vollständig. Oder: Anbieter erhält keine Kundendaten.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

C-08 Vom Nutzer ausgelöste Meldungen

Anforderung	Sendet das Produkt auf Wunsch des Nutzers Beispiele an den Anbieter (z. B. zur Verbesserung der Erkennung), dann nur so: (1) Der Nutzer löst jede Meldung selbst aus, nie automatisch und nie als Voreinstellung. (2) Das Produkt ersetzt personenbezogene Daten vorher durch erfundene Angaben gleichen Formats, ohne Zuordnungstabelle. (3) Eine Vorschau zeigt genau, was gesendet wird, und der Nutzer kann sie ändern; Wörter, die er im Original behält, bestätigt er vor dem Senden noch einmal. (4) Der Anbieter verwendet Meldungen nur zur Verbesserung des Produkts und gibt sie nicht weiter. Gilt nicht, wenn das Produkt keine Meldungen sendet.
Schwelle	**Ersetzt werden ≥ 99 % der strukturierten Kennungen (IBAN, E-Mail, Telefon, Ausweis- und Steuernummern), ≥ 98 % der Personennamen und ≥ 95 % aller Prüfwerte – wie B-03.**
Schritte	☐ 1. Meldefunktion mit Texten des Testkorpus aufrufen. ☐ 2. Gesendete Meldungen mitschneiden, nach Prüfwerten durchsuchen und die Quoten je Gruppe berechnen. ☐ 3. Prüfen, dass ohne Auslösung durch den Nutzer nichts gesendet wird und die Vorschau dem Gesendeten entspricht. ☐ 4. Vertragsbedingungen zur Verwendung prüfen.
Bestanden, wenn	Alle vier Bedingungen erfüllt und alle drei Schwellen erreicht – oder das Produkt sendet keine Meldungen.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Messwert	DE: _____ EN: _____
Belege	
Bemerkung	

Gold

G-01 Lokale Inferenz

Anforderung	Jede Inferenz für KI-Funktionen läuft auf Geräten oder Servern des Kunden (eigene Hardware oder eine Cloud-Umgebung, die der Kunde selbst kontrolliert). Keine KI-Anfrage geht an den Anbieter oder an Dritte.
Schritte	☐ 1. Installierte Modelldateien feststellen. ☐ 2. Testkorpus verarbeiten und Datenverkehr mitschneiden. ☐ 3. Mitschnitt nach Prüfwerten und KI-Anfragen durchsuchen.
Bestanden, wenn	Keine KI-Anfrage und kein Prüfwert im ausgehenden Datenverkehr.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

G-02 Offline-Betrieb

Anforderung	Alle KI-Funktionen arbeiten ohne Internetverbindung. Lizenzprüfungen und Aktualisierungen sind erlaubt, wenn sie keine Inhalte übertragen und die Verarbeitung offline mindestens 14 Tage weiterläuft.

Schwelle	**Offline-Weiterbetrieb ≥ 14 Tage.**
Schritte	☐ 1. Netzwerk trennen. ☐ 2. Testkorpus mit allen KI-Funktionen verarbeiten. ☐ 3. Systemzeit um 14 Tage vorstellen oder Herstellerangabe zur Karenzzeit prüfen.
Bestanden, wenn	Alle KI-Funktionen arbeiten offline; Karenzzeit ≥ 14 Tage.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Messwert	DE: _____ EN: _____
Belege	
Bemerkung	

G-03 Nachprüfbare Modelle

Anforderung	Modelle und Modellaktualisierungen werden als Dateien mit veröffentlichter Prüfsumme oder Signatur ausgeliefert.
Schritte	☐ 1. Prüfsumme oder Signatur einer ausgelieferten Modelldatei nachrechnen.
Bestanden, wenn	Prüfsumme bzw. Signatur stimmt.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

Silber

S-01 Vom Anbieter betriebene KI (Variante S-a)

Anforderung	KI, die personenbezogene Daten verarbeitet, läuft beim Kunden oder auf vom Anbieter betriebener Infrastruktur im EWR. Keine Dritt-KI sieht personenbezogene Daten. Modell-Dienste eines Cloud-Anbieters gelten als Dritt-KI.
Schritte	☐ 1. Hosting-Verträge und Standorte prüfen. ☐ 2. Nachweis einholen, dass der Anbieter die Modelle selbst ausführt (Konfiguration, Bereitstellung, Modelldateien). ☐ 3. Testkorpus über den Dienst verarbeiten; ausgehenden Verkehr der Anbieter-Server prüfen, soweit zugänglich, sonst Protokolle des Anbieters.
Bestanden, wenn	Modelle laufen nachweislich beim Anbieter im EWR; keine Dritt-KI erhält Prüfwerte.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

S-02 Weiche (Variante S-b)

Anforderung	Wird eine Dritt-KI eingesetzt, prüft eine Weiche beim Kunden oder auf vom Anbieter betriebener Infrastruktur jede Anfrage. Nur Anfragen ohne personenbezogene Daten gehen an die Dritt-KI.

Schritte	☐ 1. Weiche in der Architektur nachvollziehen. ☐ 2. Prüfen, dass keine Anfrage an der Weiche vorbei zur Dritt-KI gelangt.
Bestanden, wenn	Jede Anfrage an die Dritt-KI passiert die Weiche.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

S-03 Trefferquote der Weiche (Variante S-b)

Anforderung	Die Weiche hält Anfragen mit personenbezogenen Daten zuverlässig von der Dritt-KI fern.
Schwelle	**Von den Testanfragen mit personenbezogenen Daten erreichen höchstens 0,5 % die Dritt-KI (≥ 99,5 % zurückgehalten); bei Anfragen mit strukturierten Kennungen (IBAN, E-Mail, Telefon, Ausweis- und Steuernummern) höchstens 0,1 % (≥ 99,9 %).**
Schritte	☐ 1. Mindestens 1.000 Testanfragen je Sprache senden (gemischt, mit und ohne personenbezogene Daten). ☐ 2. Zählen, welche Anfragen mit Prüfwerten die Dritt-KI erreichen. ☐ 3. Quoten getrennt nach strukturierten Kennungen und übrigen Angaben berechnen.
Bestanden, wenn	Beide Schwellen erreicht, in Deutsch und Englisch.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Messwert	DE: _____ EN: _____
Belege	
Bemerkung	

S-04 Sicherer Ausfall der Weiche (Variante S-b)

Anforderung	Ist die Weiche unsicher, fehlerhaft oder nicht erreichbar, bleibt die Anfrage lokal bzw. beim Anbieter.
Schritte	☐ 1. Weiche gezielt stören (beenden, Zeitüberschreitung, fehlerhafte Antwort). ☐ 2. Prüfen, ob dabei Anfragen die Dritt-KI erreichen.
Bestanden, wenn	Bei keiner Störung erreicht eine Anfrage die Dritt-KI.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

Bronze

B-01 Pseudonymisierung vor der Übermittlung

Anforderung	Jede Anfrage an eine Dritt-KI durchläuft einen Pseudonymisierungsschritt beim Kunden oder auf vom Anbieter betriebener Infrastruktur.

Schritte	☐ 1. Pseudonymisierungsschritt in der Architektur nachvollziehen. ☐ 2. Prüfen, dass keine Anfrage daran vorbei zur Dritt-KI gelangt.
Bestanden, wenn	Jede Anfrage an die Dritt-KI wird vorher pseudonymisiert.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

B-02 Erfasste Kategorien

Anforderung	Mindestens erfasst werden: Namen natürlicher Personen, Anschriften, Geburtsdaten, Telefonnummern, E-Mail-Adressen, IBAN und Kontonummern, Ausweis-, Pass-, Steuer-, Sozialversicherungs- und Krankenversicherungsnummern, Akten- und Geschäftszeichen, Kfz-Kennzeichen, IP-Adressen. Weitere Kategorien nennt der Anbieter.
Schritte	☐ 1. Liste prüfen. ☐ 2. Je Kategorie Prüfwerte im Testkorpus verarbeiten (siehe B-03).
Bestanden, wenn	Alle Mindestkategorien erfasst.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

B-03 Erkennungsquote

Anforderung	Der Pseudonymisierungsschritt entfernt personenbezogene Daten zuverlässig. Ein Prüfwert gilt als durchgelassen, wenn er oder eine naheliegende Schreibweise davon im Klartext in der ausgehenden Anfrage steht.
Schwelle	**Entfernt werden ≥ 99 % der strukturierten Kennungen (IBAN, E-Mail, Telefon, Ausweis- und Steuernummern), ≥ 98 % der Personennamen und ≥ 95 % aller Prüfwerte insgesamt.**
Schritte	☐ 1. Mindestens 200 Testdokumente je Sprache verarbeiten. ☐ 2. Ausgehende Anfragen an die Dritt-KI mitschneiden. ☐ 3. Je Prüfwert feststellen, ob er im Klartext enthalten ist; Quoten je Gruppe berechnen.
Bestanden, wenn	Alle drei Schwellen erreicht, in Deutsch und Englisch.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Messwert	DE: _____ EN: _____
Belege	
Bemerkung	

B-04 Zuordnungstabelle bleibt

Anforderung	Die Zuordnungstabelle (Platzhalter ↔ echte Angabe) verlässt den Kunden bzw. den Anbieter nie. Die Rückführung der Platzhalter in KI-Ergebnissen geschieht beim Kunden oder beim Anbieter.

Schritte	☐ 1. Ausgehende Anfragen nach Zuordnungen durchsuchen (Platzhalter neben Prüfwert).
Bestanden, wenn	Keine Zuordnung im ausgehenden Verkehr.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

B-05 Sicherer Ausfall der Pseudonymisierung

Anforderung	Schlägt die Pseudonymisierung fehl oder ist sie nicht erreichbar, wird nichts an die Dritt-KI gesendet.
Schritte	☐ 1. Pseudonymisierung gezielt stören (beenden, Zeitüberschreitung, fehlerhafte Antwort). ☐ 2. Prüfen, ob dabei Anfragen die Dritt-KI erreichen.
Bestanden, wenn	Bei keiner Störung erreicht eine Anfrage die Dritt-KI.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

B-06 Einsicht für Nutzer

Anforderung	Nutzer können sehen, was an die Dritt-KI gesendet wurde (Vorschau vor dem Senden oder Protokoll).
Schritte	☐ 1. Vorschau bzw. Protokoll im Produkt aufrufen und mit dem Mitschnitt vergleichen.
Bestanden, wenn	Vorschau bzw. Protokoll vorhanden und vollständig.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

B-07 Vertrag mit der Dritt-KI

Anforderung	Der Vertrag mit dem Anbieter der Dritt-KI schließt Training mit den Daten aus, begrenzt die Speicherung auf höchstens 30 Tage und sieht eine Verarbeitung im EWR oder eine gültige Grundlage für die Übermittlung in Drittländer vor.
Schwelle	**Speicherung ≤ 30 Tage.**
Schritte	☐ 1. Vertrag und Konfiguration (Region, Speicherung) prüfen.
Bestanden, wenn	Kein Training, Speicherung ≤ 30 Tage, Grundlage für die Übermittlung vorhanden.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Messwert	DE: _____ EN: _____
Belege	
Bemerkung	

B-08 Richtige Bezeichnung

Anforderung	Produkt und Werbung bezeichnen pseudonymisierte Daten nicht als anonym oder anonymisiert.
Schritte	☐ 1. Produkt- und Werbetexte durchsehen.
Bestanden, wenn	Keine Bezeichnung als anonym.
Ergebnis	☐ bestanden ☐ nicht bestanden ☐ entfällt
Belege	
Bemerkung	

3 NOCIP-Index

Innerhalb der Stufe bewertet der NOCIP-Index die Umsetzung mit 0 bis 10 ganzen Punkten: fünf Gruppen zu je 0 bis 2 Punkten. Der Index ändert die Stufe nie; er steht neben ihr (z. B. „Silber · 8/10“).

Gruppe	1 Punkt / 2 Punkte	Punkte	Belege
I-1 Transparenz	1: Ein Datenflussbild ist veröffentlicht, das für jede KI-Funktion den Verarbeitungsort zeigt. 2: Zusätzlich zeigt das Produkt bei jeder KI-Funktion bzw. Anfrage, wo sie verarbeitet wird.	☐ 0 ☐ 1 ☐ 2	
I-2 Kontrolle durch den Kunden	1: Der Kunde kann jede externe KI-Verbindung abschalten; das Produkt arbeitet dann mit eingeschränkten Funktionen weiter. (Gold: erfüllt.) 2: Zusätzlich gibt es für alle KI-Funktionen eine Variante, die vollständig beim Kunden läuft. (Gold: erfüllt.)	☐ 0 ☐ 1 ☐ 2	
I-3 Datensparsamkeit	1: KI-Eingaben und -Ergebnisse werden außerhalb des Kunden höchstens 30 Tage gespeichert. (Gold: erfüllt.) 2: Zusätzlich keine Speicherung außerhalb des Kunden über die Verarbeitung hinaus, und lokale Protokolle enthalten Inhalte nur, wenn der Kunde das einschaltet.	☐ 0 ☐ 1 ☐ 2	
I-4 Integrität	1: Das Produkt prüft Signatur oder Prüfsumme jedes Modells vor dem Laden. 2: Zusätzlich sind lokale Speicher mit Inhalten oder Zuordnungstabellen verschlüsselt (oder die Einrichtung mit Betriebssystem-Verschlüsselung ist dokumentiert).	☐ 0 ☐ 1 ☐ 2	
I-5 Nachprüfbarkeit	1: Der Kunde kann ein Protokoll aller externen KI-Anfragen einsehen (Gold: aller ausgehenden Verbindungen). 2: Zusätzlich stellt der Anbieter NOCIP dauerhaft einen Testzugang bzw. eine Testinstallation für unangekündigte Stichproben bereit.	☐ 0 ☐ 1 ☐ 2	

4 Entscheidung

1. Stufe = höchste Stufe, deren Kriterien vollständig bestanden sind; alle C-Kriterien müssen bestanden sein.
2. Silber: alle Kriterien der zutreffenden Variante(n) bestanden.
3. Index = Summe der fünf Gruppen (0–10), nur innerhalb der erreichten Stufe angegeben.
4. Nicht bestandene Kriterien mit Befund in den Prüfbericht; einmalige kostenlose Nachprüfung anbieten.