NOCIP

Keine Cloud-Inferenz mit personenbezogenen Daten

Kriterienkatalog

Anforderungen und Prüfverfahren für das NOCIP-Label

Version 1.0 · 29.10.2026 · Entwurf – noch nicht freigegeben







Stufe	Bezeichnung	Bedeutung
Gold	Lokale KI	Die KI läuft beim Kunden. Echte Inhalte verlassen den Kunden nie.
Silber	Hybride KI	Personenbezogene Daten sieht nur KI des Kunden oder des Anbieters selbst.
Bronze	Pseudonymisiert	Eine Dritt-KI erhält personenbezogene Daten nur pseudonymisiert.

1 Einleitung

Dieser Katalog legt fest, welche Anforderungen ein Produkt für das NOCIP-Label erfüllen muss und wie die be next GmbH sie prüft. Er gilt für Software, die beim Kunden installiert wird, und für Software als Dienst (SaaS).

Jedes Kriterium hat eine feste Kennung: C für Kriterien aller Stufen, G für Gold, S für Silber, B für Bronze. Ein Label nennt immer die Katalogversion, nach der geprüft wurde.

Die Stufe beantwortet eine Frage: Wer betreibt die KI, die personenbezogene Daten sieht? Der NOCIP-Index bewertet zusätzlich die Umsetzung innerhalb der Stufe.

2 Begriffe

Begriff	Bedeutung
KI-Funktion	Jede Funktion des Produkts, deren Ergebnis ein maschinell gelerntes Modell erzeugt, z. B. Sprachmodelle, Erkennung von Namen, Klassifikation, Spracherkennung.
Inferenz	Die Anwendung eines Modells auf eine Eingabe, um ein Ergebnis zu erzeugen.
Kunde	Die Organisation, die das Produkt einsetzt (in der Regel der Verantwortliche im Sinne der DSGVO).
Anbieter	Das Unternehmen, das das Produkt anbietet und das NOCIP-Label beantragt.
Vom Anbieter betriebene Infrastruktur	Server, die der Anbieter selbst betreibt oder zur alleinigen Nutzung mietet, und auf denen der Anbieter die Modelle selbst installiert und ausführt (z. B. offene Modelle auf dedizierten Servern oder eigenen GPU-Instanzen).
Dritt-KI	Ein KI-Modell, das weder der Kunde noch der Anbieter selbst ausführt, sondern das über einen Dienst angesprochen wird. Dazu zählen auch Modell-Dienste eines Cloud-Anbieters im Konto des Anbieters, selbst bei Hosting in der EU.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).
Pseudonymisierung	Ersetzen personenbezogener Daten durch Platzhalter, sodass der Empfänger sie ohne die getrennt aufbewahrte Zuordnungstabelle keiner Person zuordnen kann (Art. 4 Nr. 5 DSGVO). Pseudonymisierte Daten sind nicht anonym.
Weiche	Ein Verarbeitungsschritt, der für jede Anfrage entscheidet, ob sie personenbezogene Daten enthält und wohin sie deshalb gehen darf.
Prüfwert	Erfundene personenbezogene Angabe (Name, IBAN, Anschrift …), die NOCIP in Testdokumente einsetzt, um sie im ausgehenden Datenverkehr wiederzufinden.
NOCIP-Testkorpus	Deutsche und englische Testdokumente und Testanfragen mit Prüfwerten. Er wird nicht veröffentlicht und jährlich erneuert.

3 Stufen

Gold · Lokale KI

Alle KI-Funktionen laufen auf Geräten oder Servern des Kunden. Weder der Anbieter noch Dritte erhalten Inhalte – ausgenommen Meldungen, die der Nutzer selbst auslöst und die nur erfundene Daten enthalten (C-08). Die KI-Funktionen arbeiten ohne Internetverbindung.

Silber · Hybride KI

KI, die personenbezogene Daten verarbeitet, läuft beim Kunden oder auf Infrastruktur, die der Anbieter selbst betreibt. Eine Dritt-KI erhält höchstens Anfragen ohne personenbezogene Daten. Silber hat zwei Varianten, die ein Produkt auch beide erfüllen kann.

- **S-a · Vom Anbieter betriebene KI:** Software als Dienst (SaaS), deren Modelle der Anbieter selbst betreibt.
- **S-b · Lokale KI mit Weiche:** Eine Weiche schickt nur Anfragen ohne personenbezogene Daten an eine Dritt-KI; alle anderen bleiben lokal oder beim Anbieter.

Bronze · Pseudonymisiert

Eine Dritt-KI wird eingesetzt. Vor jeder Übermittlung ersetzt ein Pseudonymisierungsschritt personenbezogene Daten durch Platzhalter. Die Zuordnungstabelle verlässt den Kunden bzw. den Anbieter nie.

4 Kriterien

4.1 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).
Nachweis	Adressen (URLs) und Bildschirmfotos der Angaben.
Prüfung	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.

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).
Nachweis	Modellverzeichnis (Tabelle in der Selbstauskunft).
Prüfung	1. Modellverzeichnis mit installierten Modelldateien, Konfiguration und beobachtetem Datenverkehr vergleichen.
Bestanden, wenn	Verzeichnis vollständig und stimmig.

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.
Nachweis	Vertragsbedingungen des Anbieters und, falls eingesetzt, der Dritt-KI; Standardeinstellungen.
Prüfung	1. Vertragsbedingungen prüfen. 2. Standardeinstellungen im Produkt prüfen.
Bestanden, wenn	Kein Training ohne ausdrückliche Einwilligung; Einwilligung standardmäßig aus.

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.
Nachweis	Beschreibung aller übermittelten Telemetrie- und Diagnosedaten.
Prüfung	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.

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.
Nachweis	Unterzeichnete Label-Vereinbarung.
Prüfung	1. Label-Vereinbarung prüfen. 2. Bei Stichproben und Verlängerung: Architektur mit dem letzten Prüfbericht vergleichen.
Bestanden, wenn	Vereinbarung unterzeichnet; keine ungemeldeten Änderungen.

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.
Nachweis	Verbindungsliste (Tabelle in der Selbstauskunft).
Prüfung	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.

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.
Nachweis	Vertragsmuster zur Auftragsverarbeitung, Liste der Unterauftragsverarbeiter.
Prüfung	1. Vertrag und Liste prüfen. 2. Liste mit Modellverzeichnis und Verbindungsliste vergleichen.
Bestanden, wenn	Vertrag vorhanden; Liste vollständig. Oder: Anbieter erhält keine Kundendaten.

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.**
Nachweis	Beschreibung der Meldefunktion, Bildschirmfotos der Vorschau, Zweckbestimmung in den Vertragsbedingungen.
Prüfung	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.

4.2 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.
Nachweis	Architekturbeschreibung; Lage der Modelldateien.
Prüfung	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.

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.**
Nachweis	Beschreibung von Lizenzprüfung und Aktualisierung.
Prüfung	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.

G-03 Nachprüfbare Modelle

Anforderung	Modelle und Modellaktualisierungen werden als Dateien mit veröffentlichter Prüfsumme oder Signatur ausgeliefert.
Nachweis	Ort der Prüfsummen bzw. Signaturen.
Prüfung	1. Prüfsumme oder Signatur einer ausgelieferten Modelldatei nachrechnen.
Bestanden, wenn	Prüfsumme bzw. Signatur stimmt.

4.3 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.
Nachweis	Architekturbeschreibung, Hosting-Verträge, Standorte.
Prüfung	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.

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.
Nachweis	Beschreibung der Weiche (Verfahren, Ort, Kategorien).
Prüfung	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.

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 %).**
Nachweis	Eigene Messwerte des Anbieters (freiwillig).
Prüfung	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.

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.
Nachweis	Beschreibung des Fehlerverhaltens.
Prüfung	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.

4.4 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.
Nachweis	Architekturbeschreibung des Pseudonymisierungsschritts.
Prüfung	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.

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.
Nachweis	Liste der erfassten Kategorien.
Prüfung	1. Liste prüfen. 2. Je Kategorie Prüfwerte im Testkorpus verarbeiten (siehe B-03).
Bestanden, wenn	Alle Mindestkategorien erfasst.

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.**
Nachweis	Eigene Messwerte des Anbieters (freiwillig).
Prüfung	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.

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.
Nachweis	Beschreibung, wo die Zuordnungstabelle gespeichert und wann sie gelöscht wird.
Prüfung	1. Ausgehende Anfragen nach Zuordnungen durchsuchen (Platzhalter neben Prüfwert).
Bestanden, wenn	Keine Zuordnung im ausgehenden Verkehr.

B-05 Sicherer Ausfall der Pseudonymisierung

Anforderung	Schlägt die Pseudonymisierung fehl oder ist sie nicht erreichbar, wird nichts an die Dritt-KI gesendet.
Nachweis	Beschreibung des Fehlerverhaltens.
Prüfung	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.

B-06 Einsicht für Nutzer

Anforderung	Nutzer können sehen, was an die Dritt-KI gesendet wurde (Vorschau vor dem Senden oder Protokoll).
Nachweis	Bildschirmfotos der Vorschau bzw. des Protokolls.
Prüfung	1. Vorschau bzw. Protokoll im Produkt aufrufen und mit dem Mitschnitt vergleichen.
Bestanden, wenn	Vorschau bzw. Protokoll vorhanden und vollständig.

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.**
Nachweis	Vertrag bzw. Vertragsbedingungen der Dritt-KI, gewählte Region.
Prüfung	1. Vertrag und Konfiguration (Region, Speicherung) prüfen.
Bestanden, wenn	Kein Training, Speicherung ≤ 30 Tage, Grundlage für die Übermittlung vorhanden.

B-08 Richtige Bezeichnung

Anforderung	Produkt und Werbung bezeichnen pseudonymisierte Daten nicht als anonym oder anonymisiert.
Nachweis	Adressen der Produkt- und Werbetexte.
Prüfung	1. Produkt- und Werbetexte durchsehen.
Bestanden, wenn	Keine Bezeichnung als anonym.

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

6 Regeln

- **Stufe:** Ein Produkt erhält die höchste Stufe, deren Kriterien es vollständig erfüllt; die gemeinsamen Kriterien (C) gelten immer. Silber gilt als erfüllt, wenn alle Kriterien der zutreffenden Variante(n) erfüllt sind.
- **Gültigkeit:** Ein Label gilt 12 Monate für die geprüfte Produktversion und deren Nachfolger ohne Änderung der KI-Architektur. Die Verlängerung erfordert eine erneute Prüfung.
- **Register:** Jedes Label erhält eine Kennung (z. B. NOCIP-G-2026-0001) und einen öffentlichen Eintrag auf nocip.com mit Produkt, Version, Stufe, Index, Katalogversion und Gültigkeit. Das Siegel des Labels trägt die Kennung als Nummer im Ring (z. B. „GEPRÜFT · NR. G-2026-0001“).
- **Aussetzen und Entzug:** Führt eine Änderung zu einer niedrigeren Stufe, wird das Label bis zur Nachprüfung ausgesetzt. Bei falschen Angaben oder Missbrauch wird es entzogen; der Entzug bleibt im Register sichtbar.
- **Kosten:** Prüfung und Label sind kostenlos. Eine Nachprüfung nach einem nicht bestandenen Kriterium ist einmal kostenlos.
- **Prüfstelle:** Die Prüfungen führt die be next GmbH durch. be next bietet mit LexITanon selbst eine Software zur Pseudonymisierung an; eigene Produkte prüft sie nach derselben Checkliste und veröffentlicht den Prüfbericht vollständig.

7 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.