Lokale KI im Haus: Architektur, Datenflüsse, Betriebsregeln

Dieses Datenblatt beschreibt Aufbau, Datenflüsse und Wartungsregeln des KI-Rechners **„Lokale KI im Haus"**, damit Datenschutzbeauftragte und IT-Verantwortliche die Lösung vor dem Pilot prüfen können. Es ist eine technische Beschreibung, ersetzt nicht die Bewertung durch den Verantwortlichen und ist keine Rechtsberatung.

ARCHITEKTUR IM ÜBERBLICK

BEREICH	AUSPRÄGUNG	HINWEIS FÜR DIE PRÜFUNG
Netz	**Eigenes WLAN** des KI-Rechners. Kein Anschluss ans Firmennetz: kein Kabel, keine IP im Firmennetz, keine Firewall-Freigabe, keine Änderung an der bestehenden IT.	Kein neues Gerät, kein neuer Port im Firmennetz. Der IT-Dienstleister muss nichts einrichten.
Internet	**Keines.** Keine Internetverbindung, keine Cloud, keine externen Schnittstellen, keine Telemetrie, keine automatischen Updates.	Keine Übermittlung an Dritte im Regelbetrieb vorgesehen, kein Abfluss über Hersteller-Dienste.
Zugriff	**Browser über interne Adresse** im WLAN des Rechners. **Zugang je Person** (persönliche Anmeldung), **Projekt je Vorgang**: getrennte Datenräume je Mandat oder Fall.	Keine Installation auf Endgeräten. Rollen, Sperren und Löschen von Zugängen durch den Kunden.
Datenhaltung	**Ausschließlich auf dem Rechner** im Büro des Kunden. Datenträger sind **Eigentum des Kunden** und bleiben auch bei Tausch oder Außerbetriebnahme im Haus.	Speicherort physisch bekannt. Sicherung nach Vorgabe des Kunden, ebenfalls ohne Internet.
Modelle	**Open-Weights-Sprachmodelle** lokal; lokale Spracherkennung (Diktate), Texterkennung (Scans), Suche über eigene Dokumente. **Kein Training** auf Kundendaten.	Eingaben verlassen den Rechner nicht. Modellstände dokumentiert, Änderung nur im Wartungsfenster.
Protokollierung	**Nachweisprotokoll je Ergebnis**: was die KI vorbereitet, was der Mensch entschieden hat. **Wartungsprotokoll je Zugriff**: wer, wann, was geändert wurde.	Beide Protokolle gehören dem Kunden; bei Gerichtsgutachten ist das Nachweisprotokoll zugleich die Offenlegung (§ 407a ZPO).
Wartung	Nur im **Fenster, das der Kunde öffnet und schließt** (Mobilfunk-Stick oder Schalter). Alternativ offline per **signiertem USB-Stick vor Ort**.	Kein dauerhafter Fernzugriff, kein Zugriff ohne Handlung des Kunden. Jeder Zugriff steht im Wartungsprotokoll.
Ersatz	**Ersatzrechner in 48 h** (Rocket Racer, Leistungsbeschreibung Stand 16.10.2026). Kundendatenträger werden übernommen oder aus der Sicherung wiederhergestellt.	Der defekte Rechner verlässt das Haus ohne Kundendatenträger.
Löschung, Rückgabe	Datenträger **verbleiben beim Kunden**. Außerbetriebnahme nach **Löschkonzept**: Löschung je Projekt oder vollständig, auf Wunsch Vernichtung der Datenträger.	Löschfristen setzt der Kunde; die Projektstruktur erlaubt Löschung je Vorgang.

ARCHITEKTURDIAGRAMM · FIRMENNETZ, LUFTSPALT, INSEL



Links das Firmennetz, das unverändert bleibt. In der Mitte der Luftspalt: keine physische oder logische Verbindung. Rechts die Insel: KI-Rechner mit eigenem WLAN, Endgeräte greifen per Browser zu. Wartung durch Rocket Racer nur im Fenster, das der Kunde öffnet (Schalter oder Mobilfunk-Stick), jeder Zugriff protokolliert; Alternative: signierter USB-Stick vor Ort, ganz ohne Verbindung.

DSGVO-EINORDNUNG · ZUR PRÜFUNG DURCH DEN VERANTWORTLICHEN · KEINE RECHTSBERATUNG

ARTIKEL	UMSETZUNG IN „LOKALE KI IM HAUS"
Art. 5 DSGVO Grundsätze der Verarbeitung	Zweckbindung durch Projekt je Vorgang; Datenminimierung: nur die vom Nutzer eingebrachten Unterlagen; Speicherbegrenzung: Löschung je Projekt nach Löschkonzept des Hauses; Vertraulichkeit: physische Trennung von Firmennetz und Internet.
Art. 25 DSGVO Technikgestaltung, Voreinstellungen	Luftspalt, kein Internet und keine Telemetrie sind Bauart, nicht Einstellung. Voreinstellung: Zugang je Person, getrennte Datenräume, kein Training auf Kundendaten.
Art. 28 DSGVO Auftragsverarbeitung	Die Verarbeitung selbst läuft vollständig auf dem Rechner des Kunden, ohne Zugriff Dritter. Rocket Racer hat nur im vom Kunden geöffneten Wartungsfenster Zugriff; dafür wird ein **AV-Vertrag für die Wartung** angeboten. Ob AV-Vertrag oder Wartungsvertrag mit Verschwiegenheitsverpflichtung, entscheidet der Verantwortliche.
Art. 30 DSGVO Verarbeitungsverzeichnis	**VVT-Vorlage wird mitgeliefert**: Zweck, Kategorien betroffener Personen und Daten, Empfänger (keine), Drittland (keines), Löschfristen (Vorgabe des Hauses), Verweis auf die TOM.
Art. 32 DSGVO Sicherheit der Verarbeitung	**TOM-Liste wird mitgeliefert**: physische Trennung, persönliche Zugänge, Protokollierung, Wartung nur im Fenster, Ersatzrechner in 48 h, Datenträger beim Kunden. Sicherung und Verschlüsselung der Datenträger werden im Pilot mit der IT des Kunden festgelegt.
Art. 35 DSGVO Datenschutz-Folgenabschätzung	**DSFA-Einschätzung wird mitgeliefert** (Datenflüsse, Risiken, Maßnahmen). Ob eine DSFA nötig ist, hängt von den Datenarten ab (z. B. Gesundheitsdaten); die Entscheidung trifft der Verantwortliche.
Art. 44 ff. DSGVO Drittlandübermittlung	**Keine Übermittlung an einen Cloud-Dienst, kein Drittland**: keine Internetverbindung, keine Cloud, keine Telemetrie, Modelle lokal. Ein TIA bewertet der Verantwortliche.

BERUFSRECHT UND ZWECKBINDUNG (KURZFASSUNG)

§ 203 StGB	Daten verlassen das Haus nicht (technische Grundlage). Wartung: schriftliche Geheimhaltungsverpflichtung. Bewertung beim Berufsträger.
§ 43e BRAO, § 62a StBerG	Vertrag mit Verschwiegenheit und Weisungsbindung für die Wartung (Vorlage wird mitgeliefert). Bewertung beim Berufsträger.
§ 11 BayGutAV	Kaufpreissammlung zweckgebunden: Ablage nur im Projekt, keine Dauerindexierung, Löschung nach Abschluss.

EU AI ACT

Art. 4 KI-Kompetenz	Schulung ist Teil des Pilots; Schulungsnachweis wird mitgeliefert, Auffrischung im jährlichen Compliance-Check (auf Wunsch).
Einstufung	Hängt vom konkreten Einsatz ab. Die Abläufe sind Vorarbeit ohne automatisierte Entscheidung; Einordnung je Ablauf in der KI-Richtlinie, Entscheidung beim Verantwortlichen.

WAS WIR DEM DSB MITLIEFERN

- ✓ **TOM-Beschreibung** (Art. 32 DSGVO)
- ✓ **VVT-Vorlage** (Art. 30 DSGVO)
- ✓ **Muster-Nachweisprotokoll** je Ergebnis
- ✓ **Wartungsprotokoll** (Muster, Einträge beim Kunden)
- ✓ **KI-Richtlinie des Hauses** mit Offenlegungsformel
- ✓ **Schulungsnachweis** (Art. 4 EU AI Act)
- ✓ **AV-Vertrag für die Wartung** (Art. 28 DSGVO)

WAS WIR NICHT TUN

- × **Kein Zugriff aufs Firmennetz:** kein Kabel, keine IP, keine Freigabe, keine Änderung an bestehender IT
- × **Kein Fernzugriff ohne Fenster:** Zugriff nur, wenn der Kunde den Schalter setzt oder den Stick steckt
- × **Kein Training** auf Kundendaten, keine Weitergabe an Modellanbieter
- × **Keine Telemetrie:** keine Nutzungsdaten, keine Fehlerberichte, keine Update-Abfragen nach außen

Mathias Matzat
Informatiker · technischer Ansprechpartner
Server, Netzwerk, Sicherheit. Fragen von IT und DSB zu Aufbau, Zugängen, Protokollen, Wartung.

Georg Matzat
KI-Consultant · Projekt und Vertrag
Beratung, Konzept, KI-Richtlinie, Schulung. Pilot, Übernahme, Betrieb.

Telefon +49 89 215577891
E-Mail georg.matzat@rocketracer.de
Web rocketracer.de/leistungen/lokale-ki/
Anfrage rocketracer.de/potenzial-check/?paket=lokale-ki