PRAXIS-LEITFADEN

Prüfkatalog für den verantwortbaren KI-Einsatz und Lovable-Bauanleitung

BVMW-Impuls · 8. Juni 2026 · Dr. Oliver Gausmann, Convios

Dieses Dokument hat zwei Teile. Teil A ist der Prüfkatalog selbst: die sechs Entscheidungen für den verantwortbaren KI-Einsatz, jeweils mit Leitfrage, Prüfpunkten, den einschlägigen Rechtsnormen und dem geforderten Nachweis. Teil B ist die Schritt-für-Schritt-Anleitung, wie Sie diesen Prüfkatalog als kleine Web-App in Lovable selbst bauen, mit Prompts zum direkten Kopieren.

Teil A · Der Prüfkatalog für den KI-Einsatz

Der Prüfkatalog besteht aus sechs Abschnitten. Jeder Abschnitt hat eine Leitfrage, vier Prüfpunkte, die einschlägigen Rechtsnormen und einen geforderten Nachweis. Beantworten Sie jeden Prüfpunkt selbst und leiten Sie aus den offenen Punkten Ihre Maßnahmen ab.

BEWERTUNGSLOGIK (FÜR ALLE ABSCHNITTE GLEICH)

Beantworten Sie jeden Prüfpunkt mit Ja, Teilweise oder Nein. Ja zählt zwei Punkte, Teilweise einen Punkt, Nein null Punkte. Je Abschnitt teilen Sie die erreichten durch die möglichen Punkte (höchstens acht je Abschnitt). Ampel je Abschnitt: grün ab 80 Prozent, gelb von 50 bis 79 Prozent, rot unter 50 Prozent. Für jeden Punkt, der nicht mit Ja beantwortet ist, ergibt sich eine konkrete Maßnahme.

Hinweis: Dieser Katalog ordnet ein und ersetzt keine Rechtsberatung. Maßgeblich ist der amtliche Wortlaut der genannten Normen.

Abschnitt 1 · Business Case · Phase: bevor Sie bauen

Leitfrage: Wollen Sie das überhaupt selbst bauen?

WORUM ES GEHT

Vor jeder Rechts- und Technikfrage steht die Wirtschaftlichkeit. Ein Eigenbau lohnt nur, wenn es keine passende Standardlösung gibt und sich der Aufwand über den ganzen Lebenszyklus rechnet.

PRÜFPUNKTE

1. Gibt es keine fertige Standardlösung, die den Bedarf abdeckt? *Falls offen: Prüfen Sie Markt und vorhandene Tools systematisch, bevor Sie selbst bauen.*

2. Rechnet sich der Eigenbau über Bau, Betrieb und Wartung auf drei Jahre? *Falls offen: Rechnen Sie die Vollkosten über drei Jahre, also Bau, Betrieb und Wartung.*

3. Ist der konkrete Nutzen benannt und messbar? *Falls offen: Halten Sie Nutzen und Erfolgskriterium schriftlich fest.*

4. Ist das Problem eng genug für eine kleine, wartbare App umrissen? *Falls offen: Verkleinern Sie den Umfang und fokussieren Sie auf einen klaren Anwendungsfall.*

RECHTSNORMEN

- Keine eigene Rechtsnorm; es ist eine Wirtschaftlichkeitsfrage.
- Die Folgeentscheidungen unterliegen jedoch DSGVO, EU AI Act, NIS2 und der Produkthaftung.

GEFORDERTER NACHWEIS

- Kurze Wirtschaftlichkeitsnotiz mit Nutzen, Vollkosten und Make-or-buy-Entscheidung.

Abschnitt 2 · Befugnis und Fähigkeit · Phase: bevor Sie bauen

Leitfrage: Dürfen und können Sie das bauen?

WORUM ES GEHT

Können und Dürfen müssen zusammenkommen. Ohne Kompetenz und ohne Freigabe der IT-Governance entsteht Schatten-KI, die niemand prüft oder absichert.

PRÜFPUNKTE

1. Liegt eine dokumentierte Freigabe der IT-Governance vor? *Falls offen: Klären Sie den Freigabeweg und holen Sie die Freigabe schriftlich ein, bevor gebaut wird.*

2. Ist die nötige fachliche Kompetenz im Team vorhanden? *Falls offen: Bauen Sie Kompetenz auf oder ziehen Sie Unterstützung hinzu.*

3. Sind die Beteiligten gemäß KI-Kompetenzpflicht geschult? *Falls offen: Holen Sie die KI-Schulung nach Artikel 4 EU AI Act nach und dokumentieren Sie sie.*

4. Ist eine erste rechtliche Einschätzung erfolgt? *Falls offen: Binden Sie Datenschutz und Recht früh ein und notieren Sie das Ergebnis.*

RECHTSNORMEN

- EU AI Act, Artikel 4 (KI-Kompetenz), gilt seit 2. Februar 2025.
- ISO/IEC 42001:2023 (KI-Managementsystem) als freiwilliger Rahmen für Schulung und Governance.
- NIS2-Umsetzungsgesetz, § 38 BSIG (Pflichten und persönliche Haftung der Geschäftsleitung); in Deutschland seit 6. Dezember 2025 in Kraft.

GEFORDERTER NACHWEIS

- Freigabedokument der IT-Governance und Schulungsnachweis.

Abschnitt 3 · Werkzeug und Tarif · Phase: während Sie bauen

Leitfrage: Welches Tool, welcher Plan?

WORUM ES GEHT

Über die Rechtskonformität entscheidet nicht die Marke. Es zählen Tarif, Vertrag, Standort und Anbieter. Für Firmendaten eignet sich nur ein Business-Tarif mit Vertrag und abgeschaltetem Training.

PRÜFPUNKTE

1. Wird ein Business- oder Enterprise-Tarif genutzt (kein Consumer)? *Falls offen: Wechseln Sie auf einen Business-Tarif, bevor Sie Firmendaten verarbeiten.*

2. Ist das Training mit eigenen Daten ausgeschaltet? *Falls offen: Deaktivieren Sie das Training mit eigenen Daten und belegen Sie es.*

3. Liegt ein Auftragsverarbeitungsvertrag (AVV) vor? *Falls offen: Schließen Sie einen AVV nach DSGVO Artikel 28 ab, sonst keine personenbezogenen Daten.*

4. Ist der Anbieter wirtschaftlich tragfähig und der Standort (möglichst EU) bekannt? *Falls offen: Prüfen Sie Anbieterbestand und Rechenzentrumsstandort und halten Sie beides fest.*

RECHTSNORMEN

- DSGVO, Artikel 28 (Auftragsverarbeitung) und Artikel 6 (Rechtsgrundlage).

- DSGVO, Artikel 44 ff. (Übermittlung in Drittländer), falls der Anbieter außerhalb der EU verarbeitet.

GEFORDERTER NACHWEIS

- AVV sowie Beleg der Tarif- und Datenschutzeinstellung.

Abschnitt 4 · Daten und Input/Output · Phase: während Sie bauen

Leitfrage: Welche Daten, und speichert die App etwas?

WORUM ES GEHT

Personenbezogene Daten dürfen Sie nur mit Rechtsgrundlage und Vertrag verarbeiten. Was nicht gespeichert wird, kann auch nicht zum Risiko werden (Client-only).

PRÜFPUNKTE

1. Werden personenbezogene Daten verarbeitet? *Falls offen: Verzichten Sie nach Möglichkeit ganz auf personenbezogene Daten.*

2. Falls ja: liegt eine Rechtsgrundlage nach DSGVO Artikel 6 vor? *Falls offen: Bestimmen und dokumentieren Sie die Rechtsgrundlage, etwa Einwilligung oder Vertrag.*

3. Speichert die App Daten, und ist das wirklich nötig? *Falls offen: Setzen Sie Datenminimierung um; vermeiden oder begründen Sie jede Speicherung.*

4. Ist der Datenfluss (Input und Output) dokumentiert? *Falls offen: Erstellen Sie eine Datenflussbeschreibung; bei Client-only genügt der Nachweis, dass nichts gesendet wird.*

RECHTSNORMEN

- DSGVO, Artikel 5 (Grundsätze: Datenminimierung Abs. 1 lit. c, Rechenschaftspflicht Abs. 2).
- DSGVO, Artikel 6 (Rechtsgrundlage), Artikel 28 (Auftragsverarbeitung), Artikel 32 (Sicherheit der Verarbeitung).

GEFORDERTER NACHWEIS

- Datenflussbeschreibung; bei Client-only ein Beleg, dass keine Daten gesendet werden.

Abschnitt 5 · Hosting · Phase: während Sie bauen

Leitfrage: Wo läuft das, wo stehen die Daten?

WORUM ES GEHT

Statisch ohne Backend ist unkompliziert. Sobald ein Server dazukommt, zählen Standort und Absicherung. Der Code sollte dem Unternehmen gehören.

PRÜFPUNKTE

1. Ist der Speicherort bekannt und möglichst in der EU? *Falls offen: Prüfen Sie den Hosting-Standort und wählen Sie eine EU-Region.*

2. Gehört der Code dem Unternehmen (Export möglich)? *Falls offen: Exportieren und sichern Sie den Code nach GitHub.*

3. Ist die Anwendung abgesichert (HTTPS, Zugriffsschutz)? *Falls offen: Aktivieren Sie Verschlüsselung und Zugriffsschutz.*

4. Bei Backend: ist es nötig, oder genügt statisch/Client-only? *Falls offen: Verzichten Sie wo möglich auf ein Backend, um Pflichten zu reduzieren.*

RECHTSNORMEN

- DSGVO, Artikel 32 (Sicherheit der Verarbeitung) und Artikel 5 (Speicherort, Integrität).

- EU AI Act, Artikel 12 (Protokollierung) und Artikel 26 (Betreiberpflichten), soweit ein Hochrisiko-System vorliegt.

GEFORDERTER NACHWEIS

- Angabe des Hosting-Standorts und Link zum GitHub-Repository.

Abschnitt 6 · Betrieb und Lebenszyklus · Phase: nachdem es läuft

Leitfrage: Wer besitzt, wartet und beendet die App?

WORUM ES GEHT

Je schneller die KI baut, desto mehr fällt von der eingebauten Prüfung weg. Der Betrieb braucht klare Rollen, sonst entsteht ein ungepflegter und haftungsträchtiger Dienst.

PRÜFPUNKTE

1. Ist ein verantwortlicher Owner benannt? *Falls offen: Legen Sie einen Owner namentlich fest und dokumentieren Sie ihn in der README.*

2. Sind Sicherheits-Patches eingeplant? *Falls offen: Vereinbaren Sie einen festen Patch-Rhythmus mit klarer Verantwortung.*

3. Gibt es einen regelmäßigen KI-Security-Lauf? *Falls offen: Terminieren Sie einen wiederkehrenden Sicherheitsscan.*

4. Ist ein klares Ende bzw. eine Abschaltung definiert? *Falls offen: Legen Sie ein Abschaltkriterium und ein Datum fest.*

RECHTSNORMEN

- Produkthaftung, Richtlinie (EU) 2024/2853: Software gilt als Produkt; anwendbar auf Produkte, die ab dem 9. Dezember 2026 in Verkehr gebracht werden.
- NIS2-Umsetzungsgesetz / § 38 BSIG (Rollen, Patch- und Meldepflichten).
- EU AI Act, Artikel 26 (Betreiberpflichten), soweit einschlägig.

GEFORDERTER NACHWEIS

- README mit Owner und Lizenz, Patch-Plan und Bericht des Security-Laufs.

Teil B · Lovable-Bauanleitung (Schritt für Schritt)

Bauen Sie die App der Reihe nach. Die Prompts unten sind zum direkten Kopieren in Lovable. Am Ende haben Sie eine veröffentlichte, client-only App, deren Code Ihnen gehört und die genau diesen Prüfkatalog abbildet.

B.0 · Vorbereitung

- Wählen Sie in Lovable oben links den Firmen-Workspace, nicht den privaten Account.
- Prüfen Sie unter Account bzw. Workspace, dass ein Business-Tarif aktiv ist.
- Schalten Sie in den Einstellungen das Training mit eigenen Daten aus, sofern vorhanden.
- Legen Sie ein neues, leeres Projekt an.

B.1 · Grundgerüst bauen

PROMPT 1 — APP ANLEGEN

```
Baue eine einseitige Web-App namens "KI-Einsatz Pruefkatalog - Selbstcheck". Zweck: Der Nutzer beantwortet sechs Abschnitte mit je vier Fragen und bekommt am Ende pro Abschnitt eine Ampel (rot/gelb/gruen), eine Punktzahl und eine Liste konkreter Massnahmen fuer alle offenen Punkte. SEHR WICHTIG: Die App laeuft ausschliesslich im Browser (client-only). Kein Backend, keine Datenbank, kein Supabase, keine Anmeldung, keine externen Netzwerkaufrufe. Es
wird nichts gespeichert und nichts gesendet. Der gesamte Zustand liegt nur im React-State und ist nach dem Schliessen weg. Sprache: durchgehend Deutsch, hoefliche Sie-Form. Design: dunkles Navy (#14263B) als Hintergrund, Gold (#FECC00) als Akzentfarbe, weisse Schrift, Karten mit abgerundeten Ecken, grosse gut lesbare Schrift. Aufbau: ein Startbildschirm mit Titel, zwei Saetzen Erklaerung und einem Button "Selbstcheck starten"; danach die sechs Abschnitte nacheinander; danach eine Ergebnisseite. Oben ein Fortschrittsbalken. Jede Frage hat drei Antwort-Buttons: Ja, Teilweise, Nein. Unten je Abschnitt "Weiter" und "Zurueck". Auf der Ergebnisseite ein Button "Zuruecksetzen".
```

B.2 · Die sechs Abschnitte mit Inhalt füllen

Dieser Prompt liefert die kompletten Inhalte. Er ist bewusst lang, damit die App genau den Prüfkatalog abbildet.

PROMPT 2 — INHALTE DER SECHS ABSCHNITTE

```
Fuelle die sechs Abschnitte mit genau diesen Titeln, Leitfragen und je vier Fragen.
Abschnitt 1 "Business Case" (Leitfrage: Wollen Sie das ueberhaupt selbst bauen?): 1) Gibt es keine fertige Standardloesung, die den Bedarf abdeckt? 2) Rechnet sich der Eigenbau ueber Bau, Betrieb und Wartung auf drei Jahre? 3) Ist der konkrete Nutzen benannt und messbar? 4) Ist das Problem eng genug fuer eine kleine, wartbare App umrissen? Abschnitt 2 "Befugnis und Faehigkeit" (Duerfen und koennen Sie das bauen?): 1) Liegt eine dokumentierte Freigabe der IT-Governance vor? 2) Ist die noetige fachliche Kompetenz im Team vorhanden? 3) Sind die Beteiligten gemaess KI-Kompetenzpflicht geschult? 4) Ist eine erste rechtliche Einschaetzung erfolgt? Abschnitt 3 "Werkzeug und Tarif" (Welches Tool, welcher Plan?): 1) Wird ein Business- oder Enterprise-Tarif genutzt, kein Consumer? 2) Ist das Training mit eigenen Daten ausgeschaltet? 3) Liegt ein Auftragsverarbeitungsvertrag (AVV) vor? 4) Ist der Anbieter wirtschaftlich tragfaehig und der Standort moeglichst in der EU? Abschnitt 4 "Daten und Input/Output" (Welche Daten, und speichert die App etwas?): 1) Werden personenbezogene Daten
```

verarbeitet? 2) Falls ja, liegt eine Rechtsgrundlage nach DSGVO Artikel 6 vor? 3) Speichert die App Daten, und ist das wirklich noetig? 4) Ist der Datenfluss aus Input und Output dokumentiert? Abschnitt 5 "Hosting" (Wo laeuft das, wo stehen die Daten?): 1) Ist der Speicherort bekannt und moeglichst in der EU? 2) Gehoert der Code dem Unternehmen, ist ein Export moeglich? 3) Ist die Anwendung abgesichert mit HTTPS und Zugriffsschutz? 4) Falls ein Backend genutzt wird, ist es noetig oder genuegt client-only? Abschnitt 6 "Betrieb und Lebenszyklus" (Wer besitzt, wartet und beendet die App?): 1) Ist ein verantwortlicher Owner benannt? 2) Sind Sicherheits-Patches eingeplant? 3) Gibt es einen regelmaessigen KI-Security-Lauf? 4) Ist ein klares Ende bzw. eine Abschaltung definiert?

B.3 · Bewertung, Ampel und Maßnahmen

PROMPT 3 — PUNKTE, AMPEL UND TO-DOS

Bewerte die Antworten so: Ja = 2 Punkte, Teilweise = 1 Punkt, Nein = 0 Punkte. Berechne je Abschnitt das Verhaeltnis aus erreichten zu moeglichen Punkten (maximal 8 je Abschnitt). Zeige je Abschnitt eine Ampel: gruen ab 80 Prozent, gelb von 50 bis 79 Prozent, rot unter 50 Prozent. Zeige auch das Gesamtergebnis mit derselben Schwelle. Auf der Ergebnisseite: pro Abschnitt eine Karte mit Ampel, Punktzahl und Prozent. Darunter ein Block "Offene Massnahmen": liste fuer jede Frage, die NICHT mit Ja beantwortet wurde, eine konkrete Handlungsempfehlung auf, gruppiert nach Abschnitt. Formuliere die Empfehlungen kurz und in hoeflicher Sie-Form, zum Beispiel: "Schliessen Sie einen Auftragsverarbeitungsvertrag nach DSGVO Artikel 28 ab, bevor Sie personenbezogene Daten verarbeiten."

B.4 · Client-only absichern und Politur

PROMPT 4 — DATENSCHUTZ UND FEINSCHLIFF

Stelle sicher, dass die App wirklich nichts speichert und nichts sendet: kein localStorage, keine Datenbank, keine API-Aufrufe, kein Tracking. Fuege unten auf der Ergebnisseite einen kleinen Hinweis hinzu: "Hinweis: Diese Auswertung laeuft nur in Ihrem Browser. Es werden keine
Daten gespeichert oder uebertragen." Mache die App responsiv und gut lesbar: grosse Schrift, klare Kontraste, ausreichend Abstand. Die Antwort-Buttons sollen den gewaehlten Zustand farbig
anzeigen (Ja gruen, Teilweise gelb, Nein rot).

B.5 · Veröffentlichen, Code sichern, Nachweis

- Klicken Sie in Lovable auf Publish, wählen Sie als Ziel lovable.app und veröffentlichen Sie.
- Exportieren Sie den Code über die GitHub-Funktion nach GitHub.
- Starten Sie den eingebauten Security- bzw. Code-Review-Lauf von Lovable.

PROMPT 5 — README MIT OWNER UND LIZENZ

Erstelle im Projekt eine README-Datei auf Deutsch mit folgenden Angaben: Projektname "KI-Einsatz Pruefkatalog - Selbstcheck"; kurze Beschreibung; Owner: Dr. Oliver Gausmann, Convios; Lizenz: MIT; Hinweis, dass die App client-only ist und keine Daten speichert; Abschnitt "Betrieb" mit den Punkten regelmaessige Sicherheits-Patches, regelmaessiger KI-Security-Lauf und geplantes Abschaltdatum.

Ergebnis

Sie haben jetzt eine veröffentlichte, client-only Web-App, die den Prüfkatalog abbildet: Sie speichert keine Daten, der Code liegt in Ihrem GitHub, ein Security-Lauf ist erfolgt und die README hält Owner, Lizenz und Betrieb fest. Damit erfüllen Sie genau die Punkte, die der Prüfkatalog in den Abschnitten 4 bis 6 verlangt.