KI-Agenten · Workflows · DSGVO

MODUL 3 — VIRTUELLES FINANCE-TEAM

3 KI-Rollen. 1 Finance-Agent. Automatisiert.

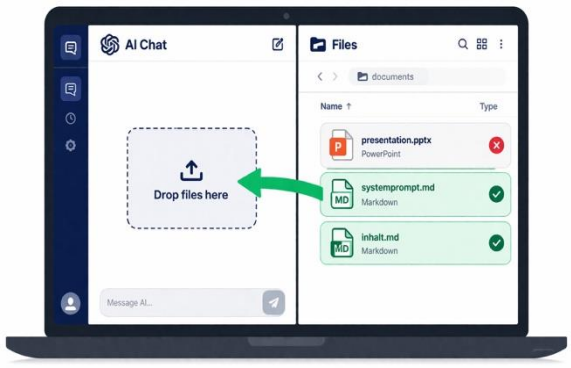
3-5 Stunden	Einzelcoaching	Live-Demo Agenten

Hinweis:

Dieses Training wird von einem KI-System als Trainer durchgeführt (z. B. ChatGPT, Gemini, Claude) – lade beide Markdown-Dateien (Systemprompt.md und inhalt.md) hoch und gib „Start“ ein. Es ist kein menschlicher Trainer erforderlich.
Download both files: https://www.foundic.org/category/schulungen/

FOUNDIC.org

1 Dateien in den Chat laden



① **Öffnen Sie Ihr LLM im Browser**
ChatGPT, Claude oder Gemini — Text-Modus (kein Audio!)

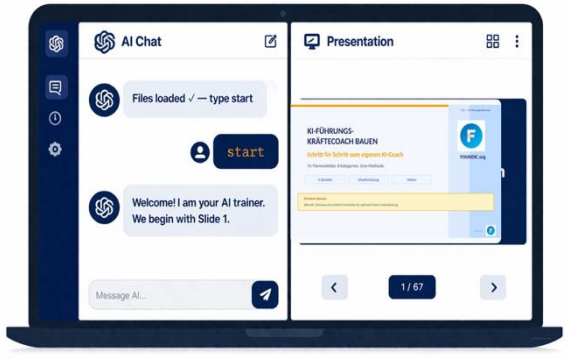
② **Beide Markdown-Dateien hochladen**
systemprompt.md + inhalt.md per Drag & Drop

✕ **Die PowerPoint NICHT hochladen**
Nur die zwei .md-Dateien gehören in den Chat

⚠ Noch KEIN Audio — Dateien nur im Text-Modus ladbar.

📥 **Dateien fehlen?** Download: foundic.org/schulungen

2 Schulung mit "start" beginnen

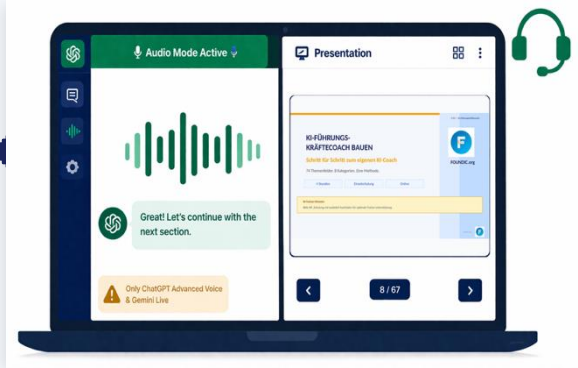


① **Tippen Sie das Wort: start**
Ein einziges Wort genügt — der Trainer startet automatisch

② **Bildschirm aufteilen**
Links: Chat-Fenster · Rechts: PowerPoint-Folien öffnen

✓ **Die Folien sind Ihr visueller Anker — der Trainer sagt Ihnen, wann Sie weiterklicken.**

3 Optional: Audio-Modus aktivieren



① **Erst Schritt 1 & 2 abschliessen**
Dateien laden + "start" eingeben — dann erst Audio

② **Audio-Modus aktivieren**
ChatGPT: Kopfhörer-Symbol · Gemini: Mikrofon-Symbol

③ **Headset aufsetzen & sprechen**
Folien betrachten, mit dem Trainer frei sprechen

Nur verfügbar in ChatGPT (Advanced Voice) und Gemini Live — nicht in Claude.

Transfer-Check Modul 2 — Was haben Sie umgesetzt?

Transfer-Check Modul 2	Was lief gut?
Welche PowerQuery-Pipeline haben Sie gebaut? Wieviel Zeit/Monat sparen Sie konkret? → Bitte kurz berichten — 2 Minuten → Erfolg feiern — dann naechsten Schritt	Welche Zeitersparnis haben Sie erreicht? → Konkrete Zahl: "X Minuten fuer Y Aufgabe" → Notieren fuer Quick-Win-Plan → Was war schwieriger als erwartet?
Einstiegs-Check Modul 3	**Ihr Automation-Problem heute**
Welcher manuelle Finance-Prozess kostet Sie am meisten Zeit? → Wir bauen dafuer heute einen Agenten-Workflow. → Trainer hoert aktiv zu — Beispiele notieren	Bitte kurz: Welchen Prozess wuerden Sie gerne automatisieren? → Wird in der Building Session aufgegriffen. → Kein Problem zu gross oder zu klein.

Dateien bereit? automation_readiness_scoring.xlsx + nordlicht_ag_datensatz.xlsx

Modul 3 startet heute. Was wir lernen, wenden wir sofort auf Ihren echten Finance-Prozess an.

Agenda — Was Sie heute erwartet

15 min	Transfer-Check M2 + Einstiegs-Check	Einstieg
10 min	Impuls: Chat zu Agenten — Paradigmenwechsel	Input
15 min	Agentic AI: Rollen + Finance-Use-Cases	Input
15 min	LIVE-DEMO: 3-Agenten-Kaskade	Demo
20 min	UEBUNG 1: Prozesse + Workflow designen	Uebung
10 min	LERNSTANDS-KONTROLLE 1 (6 Multiple-Choice)	Check
10 min	*PAUSE*	Pause
10 min	Automation-Stack: 4 Ebenen + Tool-Vergleich	Input
10 min	Guardrails, HITL-Gates + Audit-Trail	Input
15 min	Agenten-Prompt-Design + Kaskaden-Muster	Input
20 min	UEBUNG 2: Multi-Agent-Workflow bauen	Uebung
10 min	LERNSTANDS-KONTROLLE 2 (6 Multiple-Choice)	Check
10 min	*PAUSE*	Pause
40 min	BUILDING SESSION: Ihr Finance-Agent	Hands-on
15 min	Use-Cases + Mini-Case	Analyse
10 min	Abschluss-Kontrolle + Key Takeaways + Transfer	Abschluss

2–4 Stunden. 2 Lernkontrollen. 1 Building Session. 1 virtuelles Finance-Team — fertig zum Mitnehmen.

Von der Antwort zur Aktion — Was KI-Agenten anders machen

KI-Chat (Modul 1)

Sie stellen eine Frage — KI antwortet einmal.

Kein Gedaechtnis, kein Plan, keine Werkzeuge.

Output: Text. Aktion: keiner.

KI-Agent (Modul 3)

Sie geben ein ZIEL vor — Agent plant und handelt.

Nutzt Werkzeuge (Excel, API, E-Mail, Web-Search).

Output: Ergebnis + Aktion + Protokoll.

Der Unterschied in der Praxis

Chat: "Schreib mir einen Abweichungskommentar fuer EBIT -8%."

Agent: Laedt automatisch ERP-Daten, berechnet Abweichungen, schreibt Kommentar, laesst ihn pruefen, stellt ihn in das Reporting-Template ein — alles ohne Ihren Eingriff.

KI-Chat beantwortet Fragen. KI-Agent verfolgt Ziele. Das ist der Unterschied den Modul 3 macht.

Agentic AI — 3 Eigenschaften die alles aendern

Zielorientierung

Agent bekommt ein Ziel, nicht eine Anweisung. Er plant selbst wie er das Ziel erreicht.

Werkzeug-Nutzung

Agent kann externe Systeme nutzen: Excel-API, E-Mail, Web-Suche, ERP-Abfragen.

Iteratives Planen

Agent prueft seinen Output, korrigiert Fehler und wiederholt Schritte bis das Ziel erreicht ist.

Finance-Beispiel: Agent bekommt Ziel "Erstelle den monatlichen Abweichungsbericht". Er laedt ERP-Daten → berechnet Delta → schreibt Kommentar → sendet zur Freigabe. Alles ohne Ihren Eingriff.

3 Eigenschaften machen KI-Agenten zu Kollegen, nicht zu Werkzeugen: Ziel, Werkzeug, Iteration.

Wo KI-Agenten im Finance-Alltag direkt helfen

Monatsbericht-Automation Heute: 6-8 Std./Monat manuell	Mit Agent: 45 Min. + Agent-Review	**Ersparnis: ~6 Std.**
Abweichungsanalyse + Kommentar Heute: 3-4 Std./Monat	Mit Agent: 20 Min. + HITL	**Ersparnis: ~3 Std.**
Anomalie-Erkennung Buchungsjournal Heute: 2-5 Std./Monat	Mit Agent: 10 Min. + Freigabe	**Ersparnis: ~4 Std.**
Stakeholder-Reporting per E-Mail Heute: 2-3 Std./Monat	Mit Agent: 5 Min. + Freigabe	**Ersparnis: ~2.5 Std.**

Gesamt konservativ: 13-26 Std./Monat → mit Agenten-Workflows: ~2-3 Std./Monat. Das sind 3-5 Std./Woche fuer Strategie statt Routine.

Jede dieser Aufgaben koennen Sie nach Modul 3 automatisieren. Ihr Building-Session-Ergebnis ist produktionsreif.

5 Rollen — Ihr KI-gestütztes Finance-Team

Analyst-Agent

Laedt Daten, berechnet KPIs, identifiziert Abweichungen

Reviewer-Agent

Prueft Output des Analysten auf Plausibilitaet und Format

Compliance-Agent

Prueft jeden Output auf DSGVO, EU AI Act und interne Policies

Finance-Proxy-Agent

Formuliert Management-gerechten Kommentar fuer Vorstand

Eskalations-Regel

Menschlicher HITL-Gate: Controller prueft + gibt frei bei Grenzwert-Ueberschreitung

Ein virtuelles Team braucht keinen Urlaubsantrag. Es arbeitet parallel, 24/7, und eskaliert wenn noetig.

Analyst-Agent + Reviewer-Agent — Das Kern-Duo

🔍 Analyst-Agent — Scope & Prompt-Elemente

ROLLE: Finance-Analyst mit Zugriff auf ERP-Daten und KPIs.

AUFGABE: Lade [Quelle], berechne [KPI], identifiziere Top-3-Abweichungen.

OUTPUT-FORMAT: Tabelle mit Delta, %-Abweichung, Trend und 1-Satz-Kommentar.

GUARDRAIL: Kein Personenbezug. Nur aggregierte Daten. DSGVO-konform.

✅ Reviewer-Agent — Scope & Prompt-Elemente

ROLLE: Erfahrener Controller der Finance-Berichte auf Qualitaet prueft.

AUFGABE: Pruefe den Analyst-Output auf: Vollstaendigkeit, Plausibilitaet, Format.

OUTPUT-FORMAT: FREIGABE oder UEBERARBEITUNG mit konkretem Korrektur-Hinweis.

ESKALATION: Wenn Delta > 15% oder unbekannte Position: immer HITL-Gate ausloesen.

Kaskade: Analyst-Output → Reviewer-Input → Reviewer-Output → HITL-Gate → Freigabe → Endprodukt

Analyst baut. Reviewer prueft. Mensch entscheidet. Dieses Dreigestirn macht Ihre Automation sicher.

Compliance-Agent + Finance-Proxy — Sicherheit + Sprache

Compliance-Agent — Was er prueft

DSGVO: Enthaelt Output Personenbezug? Name, E-Mail, Kontonummer?→ STOPP.

EU AI Act Art. 4: KI-Literacy-Nachweis vorhanden? Audit-Trail vollstaendig?→ LOG.

Interne Policy: Verstoesst Output gegen Finance-Richtlinien? → FLAG + HITL-Eskalation.

Betragsschwelle: Wird eine Aktion ausgeloest die Betraege > 10.000 EUR betrifft?→ HITL PFLICHT.

Finance-Proxy-Agent — Management-Sprache automatisch

ROLLE: Erfahrener CFO-Berater, schreibt fuer C-Level-Publikum.

AUFGABE: Formuliere den Analyst-Output in 3 Absaetzen: Trend, Risiko, Empfehlung.

STIL: Management-gerecht, aktiv, konkret, keine Fachbegriffe ohne Erklaerung.

OUTPUT: Direkt kopierbar in Vorstandspraesentation oder Board-Report.

WICHTIG: Compliance-Agent kann einen Workflow stoppen. Finance-Proxy laeuft NACH Compliance-Freigabe. Niemals gleichzeitig.

Wann muss der Mensch eingreifen? — 3 HITL-Szenarien

Szenario 1: Betragsschwelle

Agent will eine Aktion ausloesen die Betraege > X EUR betrifft (Zahlung, Buchung, Genehmigung).
Regel: IMMER HITL-Gate. Keine Ausnahme. Betrag = Ihrem internen Limit.

Szenario 2: Unsicherheit > Schwellwert

Agent hat Konfidenz < 80% oder Abweichung > 15% ohne klar erklaerbare Ursache.
Regel: Flag setzen, Ergebnis vorhalten, Controller informieren.

Szenario 3: Externer Empfaenger

Agent will Output an externe Empfaenger (Kunden, Aufseher, Vorstand) senden.
Regel: IMMER menschlicher Review vor Versand. Keine Automation ohne Freigabe-Step.

⚡ LIVE-DEMO — Ich zeige jetzt Schritt für Schritt die 3-Agenten-Kaskade

1

1. Datenbasis:

Oeffne nordlicht_ag_datensatz.xlsx, Tab Umsatz_Q3. Aggregierter Export: 6 Monate, kein Personenbezug.

2

2. Analyst-Prompt:

ChatGPT: "Du bist Finance-Analyst. Analysiere diesen Umsatz-Export: [Tabelle einfuegen]. Berechne EBIT-Delta, Top-3-Abweichungen, 1-Satz-Kommentar je Position."

3

3. Reviewer-Prompt:

ChatGPT: "Du bist erfahrener Controller. Pruefe diesen Analyst-Output: [Output einfuegen]. Ist er vollstaendig, plausibel, managementgerecht? Gib FREIGABE oder UEBERARBEITUNG."

4

4. HITL-Gate:

Controller liest Reviewer-Output, prueft Zahlen (P-Q-R), gibt Freigabe. Dann weiter zu Finance-Proxy.

5

5. Finance-Proxy:

ChatGPT: "Du bist CFO-Berater. Formuliere aus diesem Review in 3 Absaetzen: Trend, Risiko, Empfehlung. Zielgruppe: Vorstand."

Schauen Sie zu — diese Kaskade bauen Sie in der Building Session selbst. Notizen machen ist erlaubt!

Demo-Ergebnis — P-Q-R-Check des Agenten-Outputs

Analyst-Output (Beispiel)

EBIT-Delta: -8,3% vs. Vorjahr (Plan: -5%). Haupttreiber: Energiekosten +18%, Personalkosten +4%.

Top-3: (1) Energie +156T EUR (2) Materialkosten +89T EUR (3) Reisekosten -12T EUR (Einsparung).

Reviewer-Output

FREIGABE. Output vollstaendig. Deltaberechnung korrekt. Management-Sprache OK.

Hinweis: Reisekosten sind positiv (Einsparung) — als Quick Win hervorheben in CFO-Bericht.

P-Q-R-Check des Agenten-Outputs (PFLICHT vor Freigabe)

P — Plausibilitaet:	Stimmt die Zahl -8,3%? ERP-Gegenpruefe: Ja. Trend konsistent: Ja. Keine Ausreisser.
Q — Qualitaet:	Vollstaendig? Ja. Format Tabelle? OK. Fachlich korrekt? Ja. Managementgerecht? Ja.
R — Review:	Mensch hat geprueft und unterschrieben: B. Mueller, 15.05.2025. Bereit fuer Vorstand.

KI schreibt den Bericht. Controller prueft, zeichnet ab und versetzt den Vorstand in Staunen.

ÜBUNG 1 (20 Min.) — Welche Ihrer Prozesse eignen sich fuer Agenten?

Aufgabe: Prozess-Eignung prüfen

1. Oeffnen Sie automation_readiness_scoring.xlsx, Tab Prozess-Check.
2. Listen Sie 5 wiederkehrende Finance-Aufgaben aus Ihrem Alltag.
3. Bewerten Sie jede nach 4 Kriterien (generischer Eignungscheck — Modul 4 hat vertieften 5-Kriterien AP-Check):
   Wiederholend / Regelbasiert / Datenbasiert / Pruefbar.
4. Berechnen Sie Eignungs-Score (max. 4 Punkte) — alle 4 = ideal.
5. BONUS: Analyst-Agent-Prompt fuer Top-Kandidaten skizzieren.

Orientierungshilfe: Eignungs-Kriterien (generisch, 4 Punkte — gilt für alle KI-Use-Cases)

Wiederholend: Kommt diese Aufgabe mind. monatlich vor?

Regelbasiert: Gibt es klare Regeln / Formeln / Standards?

Datenbasiert: Basiert die Aufgabe auf strukturierten Daten?

Pruefbar: Kann Reviewer-Agent Output auf Richtigkeit pruefen?

Beispiel-Ergebnisse

Monatskommentar:	**4/4 — Ideal fuer Agenten!**
Steuererklaerung:	**2/4 — Grenzfall**
Budget-Alert-Mail:	**3/4 — Gut geeignet**

Ihr Top-Prozess aus dieser Uebung wird in der Building Session zum echten Agenten. Screenshot machen!

Lernstands-Kontrolle 1 — 6 Fragen | je 1 richtige Antwort | Trainer bespricht

1. Was kennzeichnet einen KI-Agenten vs. Chat-LLM?

A) Größere Parameteranzahl
B) Autonomes Planen, Werkzeuge, Ziele — Multi-Step
C) Schnellere Antwortzeit
D) Günstigere Lizenz

2. Welche Rolle prüft den Analyst-Output auf Plausibilität?

A) Compliance-Agent
B) Finance-Proxy
C) Reviewer-Agent
D) HITL-Gate

3. Was ist ein HITL-Gate?

A) Neues KI-Modell
B) Menschlicher Freigabe-Punkt im Workflow
C) Automation-Software
D) Datenschutzstandard

4. Wann muss ein HITL-Gate ausgelöst werden?

A) Nur bei Jahresberichten
B) Bei irreversiblen Aktionen: Zahlung, ext. Versand
C) Niemals — KI ist zuverlässig
D) Nur bei >50.000 EUR

5. Was ist der Eignungs-Score 4/4 für Agenten?

A) Sehr teuer
B) Wiederholend + Regelbasiert + Datenbasiert + Prüfbar
C) Nicht automatisierbar
D) Nur für ERP-Systeme

6. Welche Daten dürfen NICHT in Cloud-KI?

A) Aggregierter Monatsumsatz
B) MAPE-Werte
C) Kontonummern + Personaldaten
D) Budgetsummen ohne Personenbezug

Kurze Pause: Alle 6 Fragen beantworten — dann besprechen wir gemeinsam.

PAUSE

 Bildschirm aus — kurz aufstehen — zurück in 10 Minuten

Nach der Pause: Automation-Stack — Welches Tool fuer welchen Finance-Prozess?

Denkaufgabe: Welchen Ihrer Prozesse aus der Uebung wuerden Sie heute noch automatisieren?

Der Automation-Stack — 4 Ebenen im Überblick

4	**Ebene 4: Agentic AI** LLM-gesteuerte Agenten-Kaskaden. Multi-Step, autonomes Planen, Feedback-Schleife.	Make AI + n8n AI + LangChain
3	**Ebene 3: Workflow-Automation** Visuelle No-Code-Workflows. Wenn-Dann-Regeln, API-Verbindungen, Benachrichtigungen.	Make.com, n8n, Zapier
2	**Ebene 2: API-Integration** Direkte Verbindung von Systemen ueber APIs. ERP + CRM + KI-Tool verbinden.	REST-API, SAP OData, Graph API
1	**Ebene 1: RPA** Regelbasierte Automatisierung ueber UI. Klick-Makros, Screen-Scraping, RPA-Bots.	UiPath, Power Automate Desktop

Modul 3 fokussiert auf Ebene 3+4. RPA und API sind Grundlagen — kein tiefes Dive heute.

Tool-Vergleich — Welches Tool fuer Finance-Controller?

Kriterium	Make.com	n8n	LangChain
Zielgruppe	Business-User Controller	Tech-affine User	Entwickler
Code noetig?	Nein — 100% No-Code	Minimal (JSON)	Ja (Python)
KI-Agenten	Native AI-Steps (Claude, GPT)	AI-Nodes vorhanden	Vollstaendiges Framework
DSGVO / On-Premise	Cloud (EU-Server)	Self-Host moeglich	Self-Host moeglich
Kosten (Paid)	Ab 9 EUR/Monat	Ca. 20 EUR/Monat (Cloud) oder Self-Host	Open Source (API-Kosten extra)
Free Tier?	✅ **1.000 Ops/Monat Fuer Einstieg reicht das**	✅ Open Source Self-Host = kostenlos	✅ Gratis API-Calls ca. 0,01–0,03 €/1k Tokens
Finance-Use-Case	Ideal fuer Controller	Gut fuer IT-nahe Teams	Fuer Entwickler-Teams
Empfehlung	★★★ **EMPFOHLEN**	★★☆ Gut	★☆☆ Entwickler

Fuer Finance-Controller ohne Programmierkenntnisse: Make.com Free Tier + ChatGPT = sofort loslegen, kein Budget noetig.

Welches Tool passt zu welchem Finance-Prozess?

Prozess	IT noetig?	Volumen	Ebene 3+?	Empfehlung
Monats-Kommentar automatisieren	Nein	mittel	✓	Make.com + ChatGPT
ERP-Export per API holen	Ja	hoch	—	Make.com + REST-API
Anomalie-Scan Buchungsjournal	Nein	hoch	✓	Make.com AI + Excel
Stakeholder-E-Mail generieren	Nein	niedrig	✓	Make.com + GPT-4o
Compliance-Report an Aufsicht	Ja	niedrig	✓	n8n Self-Host + GPT
Dashboard-Refresh aus ERP	Ja	hoch	—	Power Automate + API

Keine IT? Keine API? Kein Problem. Make.com loest 80% aller Finance-Automation-Faelle ohne Code.

4 Guardrail-Muster die jeden Finance-Agenten sichern

Output-Validation
Agent prueft Output selbst gegen definierte Regeln BEVOR er ihn weitergibt.
Beispiel: "Enthaelt Output eine Zahl ausserhalb des plausiblen Bereichs? STOPP."

Data-Masking
Agenten-Input wird automatisch bereinigt: keine Kontonummern, keine Namen, keine Adressdaten.
Beispiel: Regex-Filter im Make.com-Step vor dem KI-Aufruf.

Konfidenz-Schwellwert
Agent schaltet HITL-Gate wenn Konfidenz-Score < 80% oder Abweichung > definierbarer Grenze.
Beispiel: GPT-Antwort mit Konfidenz-Tag auswerten.

Audit-Trail (EU AI Act)
Jeder Agenten-Aufruf wird geloggt: Zeitstempel, Input-Hash, Output-Hash, User-ID, Freigabe.
EU AI Act Art. 4+26 verlangt das fuer High-Risk-Systeme.

HITL-Gates richtig einbauen — 3 Implementierungsmuster

🤝 Muster 1: Approval-Step in Make.com

Workflow pausiert nach Agenten-Output.

Make sendet E-Mail an Controller mit 2 Buttons: FREIGABE / ABLEHNUNG.

Controller klickt Button — Make.com setzt Workflow fort oder bricht ab.

Einrichtungszeit: ca. 30 Minuten. Kein Code noetig.

📊 Muster 2: Review-Formular

Workflow generiert Output + PDF-Zusammenfassung.

Controller erhaelt Link zu Review-Formular (Google Form oder Typeform).

Formular-Antwort triggert naechsten Workflow-Step.

Vorteil: Revisions-Kommentar kann direkt eingetragen werden.

🚨 Muster 3: Eskalations-Slack / Teams-Nachricht

Workflow sendet kritischen Output in dedizierten Slack/Teams-Kanal.

Controller schreibt "OK" oder "STOPP" als Reply.

Make.com watched den Kanal und reagiert auf die Antwort.

Vorteil: Mobil genehmigen, kein separates Tool noetig.

EU AI Act 2025 — Was Finance-Controller wissen müssen

Art. 4	**KI-Kompetenz-Pflicht** 10B981
Art. 13	**Transparenz-Pflicht** 3B82F6
Art. 26	**HITL-Pflicht (High-Risk)** 8B5CF6
Audit-Trail	**Praktische Umsetzung** F59E0B

EU AI Act: Kein Grund zur Panik. Dokumentieren, kennzeichnen, HITL — das tun Sie ab heute sowieso.

DSGVO-Regeln fuer KI-Agenten im Finance-Alltag

Darf NICHT in Cloud-KI (ChatGPT, Claude, etc.)

Personenbezogene Daten: Name, E-Mail, IBAN, Steuernummer, Kontonummer.

Mitarbeiterdaten: Gehalt, Beurteilungen, Anwesenheit.

Kundendaten: Vertragsinhalte mit Personenbezug, Kreditwuerdigkeitsdaten.

Grauzone — nur mit vertraglicher Absicherung

Aggregierte Finanzdaten ohne Personenbezug (z.B. Umsatz nach Produktgruppe) — meist ok.

Anonymisierte Benchmarks und KPI-Berichte — meist ok, pruefen lassen.

E-Mails an Geschaeftspartner — nur wenn Auftragsverarbeitungsvertrag mit KI-Anbieter besteht.

Sicher ohne Einschraenkung

Oeffentliche Marktdaten (Boersenkurse, Branchenberichte, Zinssaetze).

Interne Prozessbeschreibungen und Workflow-Dokumentation ohne Personenbezug.

Anonymisierte historische Daten und aggregierte Forecasts ohne Personenbezug.

ÜBUNG 2 (20 Min.) — Designen Sie Ihren eigenen Finance-Agent-Workflow

Aufgabe in 4 Schritten

Schritt 1: Nehmen Sie Ihren Top-Prozess aus Uebung 1 (Score 3+/4).

Schritt 2: Definieren Sie Eingang (Input), Agenten-Schritte, Ausgang (Output).

Schritt 3: Markieren Sie: Wo braucht der Workflow ein HITL-Gate?

Schritt 4: Pruefe: Enthaelt der Input DSGVO-rote Daten? Wenn ja: Bereinigungsschritt einbauen.

Vorlage: Workflow-Skizze

TRIGGER: Wann startet der Workflow? (Zeit / Datei-Eingang / manuell)

INPUT: Welche Daten? Aus welchem System? DSGVO-Kategorie?

AGENT 1: Was tut er? Prompt-Skizze in 2 Saetzen.

AGENT 2 (optional): Reviewer / Compliance.

HITL-GATE: Wer genehmigt? Wie? (E-Mail / Teams / Formular)

OUTPUT: Was kommt raus? In welchem Format?

Tipp: Legen Sie Ihren Workflow-Entwurf bereit — er wird in der Building Session direkt umgesetzt!

Lernstands-Kontrolle 2 — 6 Fragen | je 1 richtige Antwort | Trainer bespricht

1. Was macht ein Guardrail-Muster?

A) Verbessert LLM-Modell
B) Schützt Output vor unkontrollierten Ergebnissen
C) Senkt Cloud-Kosten
D) Automatisiert Freigaben

2. DSGVO: Was darf NICHT in Cloud-KI?

A) Aggregierter Monatsumsatz
B) IBAN, Name, Steuernummer
C) Anonymisierte Benchmarks
D) Öffentliche Marktdaten

3. EU AI Act Art. 4 verlangt:

A) Vollständiges KI-Verbot
B) Angemessene KI-Kompetenz der Nutzer
C) Technische Zertifizierung
D) Externe Audits alle 2 Jahre

4. Was ist Data-Masking im Agenten-Workflow?

A) Datei-Verschlüsselung
B) Entfernung sensibler Daten vor KI-Aufruf
C) UI-Overlay für Datenschutz
D) Cloud-Backup-Verfahren

5. Wann ist ein Audit-Trail Pflicht?

A) Nie — freiwillig
B) Bei KI-generierten Entscheidungen (EU AI Act)
C) Nur bei Jahresabschluss
D) Nur bei Personaldaten

6. HITL-Approval-Step in Make.com — wie funktioniert es?

A) KI genehmigt selbst
B) Controller klickt E-Mail-Button — Workflow setzt fort
C) Automatische Timer-Freigabe nach 24h
D) Supervisor muss Code eingeben

Kurze Pause: Alle 6 Fragen beantworten — dann besprechen wir gemeinsam.

PAUSE

 Bildschirm aus — kurz aufstehen — zurück in 10 Minuten

Nach der Pause: Building Session — Ihr Finance-Agent entsteht jetzt!

Halten Sie Ihren Workflow-Entwurf aus Uebung 2 bereit.

🏗️ BUILDING SESSION (40 Min.) — Heute bauen Sie Ihren ersten Finance-Agenten. Kein Demo — Ihre echten Daten.

1	🎯 Schritt 1: Rollen + I/O definieren
2	📐 Schritt 2: Workflow-Diagramm zeichnen
3	🔍 Schritt 3: Analyst-Prompt formulieren
4	✅ Schritt 4: Reviewer-Prompt formulieren
5	▶️ Schritt 5: Agenten-Kaskade testen
6	🤝 Schritt 6: HITL-Gate definieren + QC-Checkliste

✅ Am Ende haben Sie: Analyst-Prompt + Reviewer-Prompt + HITL-Gate-Spezifikation — sofort einsetzbar.

Keine Demo mehr — jetzt bauen Sie. Ihr eigener Prozess. Ihre Daten. Ihr Agent. Los.

1 Schritt 1: Rollen + I/O definieren

🎯 Aufgabe: Definieren Sie Ihren Agenten-Workflow

A) WAS ist der Input? (Welche Datei / welcher Datenbankexport / API-Quelle?)

B) WAS ist der gewuenschte Output? (Format, Laenge, Zielgruppe)

C) Welche Agenten-Rolle ist noetig? (Analyst / Reviewer / Finance-Proxy / Compliance)

D) Wer ist der HITL-Gate-Entscheider? (Name oder Rolle)

📝 Vorlage: Ihre Workflow-Karte

PROZESS-NAME: _____

INPUT (DSGVO-Kategorie Rot/Gelb/Gruen): _____

GEWUENSCHTER OUTPUT: _____

AGENTEN-ROLLEN: _____

HITL-GATE-PERSON: _____

5 Minuten. Workflow-Karte ausfuellen. Das ist das Fundament Ihres Agenten.

2 Schritt 2: Workflow-Diagramm zeichnen

TRIGGER	Wann startet? (Zeit / manuell / Datei-Upload)
INPUT-SCHRITT	Datei laden + DSGVO-Masking (falls noetig)
ANALYST-AGENT	Aufgabe + Prompt-Skizze + Output-Format
REVIEWER-AGENT	Pruefregel + Eskalations-Schwelle
HITL-GATE	Wer genehmigt? Wie? (E-Mail / Teams / Formular)
OUTPUT	Format + Empfaenger + Archivierung

Zeichnen Sie die Boxen — mit Pfeilen. Papier oder Notizblock. 5 Minuten.

3 Schritt 3: Analyst-Prompt formulieren

🔍 Analyst-Prompt: CRAFT-Struktur (aus Modul 1)

C — Kontext: Du bist Finance-Analyst der [Firmenart] mit Fokus auf [Bereich].

R — Rolle: Analysiere praezise, zahlenbasiert, ohne Annahmen ausserhalb der Daten.

A — Aufgabe: [Konkrete Aufgabe — z.B. "Berechne EBIT-Delta Q3 vs. VJ"].

F — Format: Tabelle mit Delta, %, Trend-Pfeil, 1-Satz-Kommentar je Position.

Beispiel-Prompt (Nordlicht AG)

Du bist Finance-Analyst der Nordlicht AG. Analysiere den folgenden Umsatz-Export:
[Tabelle hier einfuegen]
Berechne: (1) EBIT-Delta Q3 vs. Vorjahr in EUR und %. (2) Top-3-Abweichungspositionen. (3) 1-Satz-Kommentar je Position.
Format: Tabelle. Kein Personenbezug. Nur aggregierte Daten.

Schreiben Sie Ihren Analyst-Prompt jetzt. CRAFT-Struktur als Checkliste. 6 Minuten.

4 Schritt 4: Reviewer-Prompt formulieren

✅ Reviewer-Prompt: Pruefliste + Eskalation

R1 — Vollstaendigkeit: Sind alle geforderten Felder / KPIs im Analyst-Output enthalten?

R2 — Plausibilitaet: Liegt eine Zahl ausserhalb des erwarteten Bereichs? (>20% Abweichung: FLAG)

R3 — Format: Stimmt das geforderte Format (Tabelle, Saetze, Laenge)?

R4 — Eskalation: Wenn eine Regelabweichung → antworte mit: "UEBERARBEITUNG: [Hinweis]"

Beispiel-Prompt (Nordlicht AG)

Du bist erfahrener Controller. Pruefe den folgenden Analyst-Output auf:
1. Vollstaendigkeit (alle 3 KPIs vorhanden?)
2. Plausibilitaet (kein Delta > 30% ohne Erklaerung?)
3. Format (Tabelle korrekt strukturiert?)
Gib entweder: FREIGABE oder UEBERARBEITUNG: [konkreter Hinweis].
Analyst-Output: [Output hier einfuegen]

5 Schritt 5: Agenten-Kaskade testen

JETZT TESTEN: Fuehren Sie Ihren Analyst-Prompt + Reviewer-Prompt in ChatGPT aus

Test-Input	Oeffnen Sie nordlicht_ag_datensatz.xlsx Tab Umsatz_Q3. Kopieren Sie die Tabelle (ohne Personenbezug).
Analyst	Fuegen Sie Test-Input + Ihren Analyst-Prompt in ChatGPT ein. Dokumentieren Sie Output.
Reviewer	Fuegen Sie Analyst-Output + Ihren Reviewer-Prompt in ChatGPT ein. Erhalten Sie FREIGABE?
P-Q-R-Check	Pruefen Sie Output: Plausibilitaet, Qualitaet, Richtigkeit. Notieren Sie was noch fehlt.

Testen Sie. Jetzt. Live. 10 Minuten. Ich bin da wenn der Reviewer nicht "FREIGABE" sagt.

6 Schritt 6: HITL-Gate definieren + QC-Checkliste

HITL-Gate spezifizieren

A) Wer genehmigt? Name + Rolle: _____

B) Wie wird der Output uebermittelt? (E-Mail / Teams / Formular): _____

C) Was passiert bei ABLEHNUNG? (Workflow-Abbruch / Ueberarbeitung + Retry): _____

D) Timeout-Regel: Wenn keine Antwort in X Stunden → automatisch eskalieren an: _____

QC-Checkliste: Ist Ihr Agent fertig?

- ☐ Analyst-Prompt: CRAFT-Struktur vollstaendig?
- ☐ Reviewer-Prompt: FREIGABE / UEBERARBEITUNG klar definiert?
- ☐ HITL-Gate: Person + Methode festgelegt?
- ☐ DSGVO: Input DSGVO-konform (kein Personenbezug)?
- ☐ Audit-Trail: Wo wird der Agenten-Output gespeichert/protokolliert?
- ☐ Test bestanden: Reviewer hat FREIGABE gegeben?

Alle 6 Checkboxen abgehakt? Dann haben Sie heute einen produktionsreifen Finance-Agenten gebaut. Herzlichen Glueckwunsch!

Building Session abgeschlossen — Was haben Sie gebaut?

Bitte kurz vorstellen (2 Min. je Teilnehmer): Prozess + Agent + HITL-Gate + 1 Lernmoment

🔍 Bernds Ergebnis (Beispiel)

Prozess: Monatlicher EBIT-Abweichungskommentar fuer Nordlicht AG.

Analyst-Agent: CRAFT-Prompt mit ERP-Export als Input. Output: Tabelle + Kommentar.

Reviewer-Agent: 5 Pruefregel, Eskalation bei >20% Delta.

HITL-Gate: Teams-Nachricht an Bernd Mueller — Freigabe per Reply.

Zeitersparnis geschaetzt: 4-5 Stunden pro Monat.

📧 Tanjas Ergebnis (Beispiel)

Prozess: Budget-Alert-E-Mail an Stakeholder bei EBIT-Abweichung > 10%.

Agent: GPT-4o formuliert E-Mail nach Vorlage.

HITL-Gate: E-Mail-Approval vor Versand. DSGVO: kein Personenbezug im Prompt.

Lernmoment: Data-Masking-Step vor KI-Aufruf war entscheidend.

Fantastisch! Zwei Finance-Agenten in 40 Minuten. Das ist der Modul-3-Moment.

6 Finance-Agenten-Use-Cases die heute schon in der Praxis laufen

Monatsbericht-Automation

Analyst laedt ERP, berechnet KPIs, Reviewer prueft, Finance-Proxy formatiert fuer Vorstand.

Zeitersparnis: 5-7 Std./Monat

Anomalie-Erkennung Buchungsjournal

Agent scannt saemtliche Buchungen auf Abweichungen >2σ, meldet an Controller.

Zeitersparnis: 3-4 Std./Monat

Intercompany-Abstimmung

Agent vergleicht IC-Positionen beider Entitaeten, erstellt Differenzliste, eskaliert.

Zeitersparnis: 4-6 Std./Monat

Cashflow-Forecast-Update

Agent laedt IST-Zahlen, aktualisiert Forecast-Modell, erlaeutert Top-3-Treiber.

Zeitersparnis: 2-3 Std./Monat

Stakeholder-Reporting

Agent erstellt personalisierte Berichte fuer CFO, Board und Investoren aus gemeinsamer Datenbasis.

Zeitersparnis: 3-5 Std./Monat

Compliance-Pre-Check

Agent prueft Buchungen auf Richtlinienkonformitaet BEVOR Monatsabschluss. Reduziert Nacharbeiten.

Zeitersparnis: 2-4 Std./Monat

Diese 6 Use-Cases decken 80% aller Finance-Routine-Aufgaben ab. Was davon bauen Sie als naechstes?

MINI-CASE: Nordlicht AG — Ein Agenten-Workflow in der Krise

Situation: Freitagabend, 18:00 Uhr. CFO braucht Bericht bis Montag 8:00 Uhr.

Bernd Mueller, Controller bei Nordlicht AG, bekommt Freitag um 18:00 Uhr eine Teams-Nachricht:

"Bernd — brauche Montag 8:00 Uhr den vollstaendigen Q3-Abweichungsbericht fuer den Aufsichtsrat.

"5 Entitaeten. EBIT, Cashflow, Working Capital. Mit Kommentar und Trend-Analyse."

Bernd denkt: Normalerweise 2 Tage Arbeit. Mit seinem neuen Agenten-Workflow?

Er hat: ERP-Export (aggregiert, DSGVO-konform), seinen Analyst-Prompt aus der Building Session,

seinen Reviewer-Prompt, HITL-Gate via Teams, und... 3 Stunden Zeit heute Abend.

Aufgabe: Was tut Bernd? Schritt fuer Schritt.

1. Prueft Bernd den Input zuerst auf DSGVO? 2. Welchen Agenten startet er zuerst?
3. Was tut er wenn der Reviewer "UEBERARBEITUNG" sagt? 4. Wann schickt er an den CFO?

Sie haben 2 Minuten. Was wuerden Sie in Bernds Situation tun? Denken Sie laut.

Bernds Workflow — Schritt fuer Schritt

18:05	🟢 DSGVO-Check: ERP-Export prueft. Aggregiert, kein Personenbezug. Gruen.
18:10	🔍 Analyst-Agent: CRAFT-Prompt + ERP-Tabelle in ChatGPT. 5 Entitaeten, 3 KPIs. Output in 4 Min.
18:20	⚠️ Reviewer-Agent: Output in Reviewer-Prompt. Ergebnis: "UEBERARBEITUNG: Working Capital Entitaet 3 fehlt."
18:28	✅ Bernd korrigiert: Entitaet 3 Daten nachgeladen, Analyst erneut. Reviewer: "FREIGABE".
18:35	🤝 HITL-Gate: Bernd prueft Zahlen persoenlich (P-Q-R-Check). Zeichnet ab.
18:42	📋 Finance-Proxy: Managementkommentar fuer Aufsichtsrat. Board-sprache, 3 Absaetze.
18:50	📨 Bernd sendet Teams-Nachricht an CFO: "Bericht liegt bereit — Frueher als erwartet."

✅ Fazit: 45 Minuten statt 2 Tage. Bernd schlaeft gut. Der Aufsichtsrat bekommt seinen Bericht.

Das ist kein Zukunftsszenario. Das koennen Sie ab Montag. Mit dem was Sie heute gebaut haben.

MINI-CASE 2: Tanja + Budget-Alert — Was geht schief?

Tanjas Workflow

Tanja baut Budget-Alert-E-Mail-Workflow.

Bei EBIT-Abweichung >10%: Agent formuliert E-Mail an Investoren.

Workflow soll E-Mail automatisch versenden.

Keine Data-Masking-Step. Investor-E-Mail-Adressen im Prompt. Kein HITL-Gate vor Versand.

Erste E-Mail geht raus: "Sehr geehrter Herr Mustermann, Ihr Portfolio zeigt -12%..."

Was ist falsch?

DSGVO-Verstoß: Investoren-Namen und E-Mail-Adressen im Prompt = Personenbezug in Cloud-KI.

Kein HITL-Gate: E-Mail direkt an externe Empfaenger ohne menschlichen Review = High-Risk.

Keine Freigabe: Automatisch versendete Stakeholder-Kommunikation = Haftungsrisiko.

Richtige Loesung: Data-Masking + HITL-Gate + Freigabe vor Versand

Investor-IDs statt Namen im Prompt. E-Mail-Entwurf per HITL-Gate freigeben. Erst danach automatisch versenden.

Abschluss-Check: 6 Fragen — Modul 3 komplett. Je 1 richtige Antwort.

1. Was ist Agentic AI im Vergleich zu Chat-LLM?

A) Günstigeres Modell
B) Autonomes, zielorientiertes KI-System mit Werkzeug-Nutzung
C) Neue OpenAI-Version
D) Sprachmodell mit größerer Datenmenge

2. Welche Rolle gibt die finale Freigabe vor dem Finance-Proxy?

A) Analyst-Agent
B) Compliance-Agent
C) Reviewer-Agent mit HITL-Bestätigung
D) CFO direkt

3. Was bedeutet Make.com-Approval-Step?

A) Automatische Freigabe nach 24h
B) Controller klickt E-Mail-Link: FREIGABE oder ABLEHNUNG
C) KI-Selbstprüfung
D) API-Zertifizierung

4. Welche Daten sind DSGVO-sicher für Cloud-KI?

A) IBAN und Kontonummer
B) Aggregierter Umsatz ohne Personenbezug
C) Mitarbeitergehalt
D) Kundenadressen

5. EU AI Act Art. 26 gilt für:

A) Alle KI-Nutzungen
B) High-Risk-KI die Entscheidungen beeinflusst
C) Nur Gesundheitsdaten
D) Nur staatliche Systeme

6. Was sind die 3 HITL-Trigger?

A) Länge + Format + Ton
B) Betrag + Unsicherheit + Externer Versand
C) Nur bei Fehlern
D) Nur bei Jahresabschluss

Alle 6 richtig? Modul 3 abgeschlossen. Modul 4 baut auf Ihrem Agenten-Workflow auf.

5 Dinge die Sie heute mitnehmen

1. **Agenten vs. Chat:**
   KI-Agenten verfolgen Ziele, nutzen Werkzeuge und planen iterativ — Chat-LLM antwortet nur einmal. Das ist der fundamentale Unterschied.
2. **Virtuelles Finance-Team:**
   Analyst + Reviewer + HITL-Gate = das Minimale. Compliance + Finance-Proxy = das Vollstaendige. Building Session: Ihr Agent ist fertig.
3. **Automation-Stack:**
   Make.com (Ebene 3+4) ist das richtige Tool fuer Finance-Controller ohne IT-Unterstuetzung. No-Code, EU-Server, native KI-Integration.
4. **Guardrails + DSGVO:**
   Data-Masking, Output-Validation, Konfidenz-Schwellwert, Audit-Trail — keine Optional, sondern Pflicht. Rote Daten bleiben lokal.
5. **HITL ist nicht Schwaeche:**
   Human-in-the-Loop ist kein Engpass — es ist Ihr Schutzschild. Geld, Unsicherheit, externer Versand = immer menschlicher Gate.

Diese 5 Punkte sind das Fundament Ihres virtuellen Finance-Teams. Sie sind bereit fuer Modul 4.

Transfer-Aufgabe — Wählen Sie eine Option

A

Option A: Analyst-Kaskade produktiv

Setzen Sie Ihren Building-Session-Agenten in die Praxis um.
Naechster echte Bericht: Agenten-Workflow verwenden, Ergebnis dokumentieren.

- Datum: naechster Monatsbericht
- Protokoll: Agent-Output + Reviewer-Ergebnis + Freigabe-Zeitstempel
- Ziel: vollstaendiger P-Q-R-Check

B

Option B: Make.com-Account einrichten

Richten Sie Make.com Free Tier ein und bauen Sie Ihren Building-Session-Workflow als echten Make-Workflow.
Keine Programmierung noetig.

- Make.com-Account anlegen (kostenlos)
- Analyst-Prompt als "ChatGPT"-Modul konfigurieren
- HITL-Approval per E-Mail einbauen

C

Option C: Audit-Trail + Governance-Dokumentation

Erstellen Sie ein einfaches Governance-Dokument fuer Ihren Finance-Agenten:
Zweck, Datenfluss, Guardrails, HITL-Regeln, Audit-Log-Schema.

- Vorlage: ai_governance_pack_vorlage.docx aus Modul 1
- EU AI Act Art. 4 Nachweis einbauen
- Vom Vorgesetzten unterschreiben lassen

Alle drei Optionen produzieren produktionsreife Ergebnisse. Wählen Sie was zu Ihrem nächsten Schritt passt.

Digital Finance Masterclass — Ihr Fortschritt

Der Masterclass-Fahrplan

1	**Einstieg & Quick Wins** *KI-Grundlagen, CRAFT, Datenschutz, Custom GPT*	✅ Abgeschlossen
2	**Data Analytics** *PowerQuery, KPI-Dictionary, Forecasting, IBCS*	✅ Abgeschlossen
3	**Virtuelles Finance-Team** *Agenten, Make.com, Guardrails, HITL*	✅ Abgeschlossen
4	**Accounting & & Operations** *RAG, AP-Automation, Fraud-Erkennung, SoD*	→ Nächste Sitzung
5	**Strategie & Governance** *EU AI Act, ROI-Rechner, Roadmap, Change*	→ Abschluss

Mein Quick-Win-Plan — ab morgen

1. **Mein Workflow:**
   Agent-Kaskade für einen Finance-Use-Case bauen
2. **Automation-Scan:**
   Readiness-Score für Top-3-Prozesse ausfüllen
3. **Mein HITL-Gate:**
   Kritischen Prüfschritt vor KI-Ausgabe definieren
4. **Governance starten:**
   ai_governance_pack_vorlage.docx — Bausteine B1–B2

3 von 5 Modulen abgeschlossen. Nächste Session: Accounting & Operations.

Quick-Win-Worksheet — Ihre Massnahmen bis zur nächsten Session

1	**Mein Building-Session-Ergebnis** Prozess-Name + Agenten-Konfiguration:
2	**Transfer-Option (A/B/C)** Gewaehlt: _____. Deadline: _____
3	**Make.com-Step** Account angelegt bis: _____
4	**HITL-Gate konfiguriert** Person: _____. Methode: _____
5	**Erster echter Agent-Lauf** Geplant fuer: _____
6	**Governance-Dokument** Gestartet: ____. Fertig bis: _____

Ziel: Bis Modul 4 mindestens 1 echter Agent-Lauf mit dokumentiertem Ergebnis.

Modul 3 abgeschlossen!

Virtuelles Finance-Team — gebaut, getestet, bereit.

Modul 4: Accounting Ops

Buchungsautomation · Periodenabschluss mit KI · Matching + Reconciliation

Glossar — Schluessel-Begriffe Modul 3

Begriff	Erklaerung
Agentic AI	KI-System das Ziele verfolgt, Werkzeuge nutzt und iterativ plant. Nicht nur Textantworten.
Analyst-Agent	LLM-Rolle die Daten laedt, KPIs berechnet und strukturierte Outputs erstellt.
Reviewer-Agent	LLM-Rolle die Outputs prueft: Vollstaendigkeit, Plausibilitaet, Format. Gibt FREIGABE oder FLAG.
HITL-Gate	Human-in-the-Loop Gate: Menschlicher Freigabe-Schritt vor irreversiblen Aktionen.
Make.com	No-Code-Workflow-Automation-Tool. Verbindet APIs und KI-Modelle ohne Programmierung.
Guardrail	Sicherheitsregel fuer Agenten: Output-Validation, Data-Masking, Konfidenz-Schwelle.
Audit-Trail	Protokoll jedes KI-Aufrufs: Zeitstempel, User, Modell, Input-Hash, Output-Hash, Freigabe.
EU AI Act Art. 4	Kompetenz-Pflicht: Nutzer von KI muessen angemessene KI-Kompetenz nachweisen.
Data-Masking	Entfernen personenbezogener Daten aus KI-Inputs. Pflicht bei DSGVO-Grauzone.
P-Q-R-Check	Plausibilitaet + Qualitaet + Review: Menschliche Endpruefung vor Freigabe jedes KI-Outputs.

Du hast es geschafft! 

Danke für Deine Zeit und Dein Vertrauen.

Ich hoffe, du hast etwas mitgenommen — und setzt es schon morgen ein.

Verbesserungsvorschläge? Hinterlasse einen Kommentar auf foundic.org — wir lesen jeden Hinweis und optimieren unsere Schulungen laufend.

Unser Ziel: Kostenlose Schulungen für alle — denn Weiterbildung sollte keine Frage des Budgets sein.

Wenn dir die Schulung gefallen hat — lade uns auf einen Kaffee ein. Das hilft uns, weitere kostenlose Schulungen zu entwickeln.

Lade uns auf einen Kaffee ein

-

→ Feedback & Kommentar: foundic.org/schulungen