DAXAIS
Struktur für Sicherheit. Klarheit für KI.

KI, N8N, GOVERNANCE, WORKFLOW

KI-Workflow in n8n: Praxisleitfaden für Governance & Sicherheit

Strukturierte Arbeitshilfe für sichere und nachvollziehbare KI-Workflows in n8n; für Governance-Verantwortliche.

Struktur für Sicherheit. Klarheit für KI.

Zielgruppe: Fachkräfte KI-Governance, Datenschutzbeauftragte, Prozessmanager KI & Compliance

Stand August 2026

ORIENTIERUNG

Worum es geht

Der Leitfaden unterstützt Sie dabei, in n8n belastbare KI-Workflows zu planen, zu dokumentieren und an zentralen Governance-Anforderungen (SDM 3.1 D3.2.1) nachweisbar abzusichern.

NAVIGATOR

Drei Orientierungspunkte

9 Kriterien

EDSA-Check für hohes Risiko

Art. 35 DSGVO

Vorprüfung nach Datenschutzgesetz

n8n Workflows

Modulare Open-Source Automation

PROCESS

1. Aufgaben klären und Workflows strukturiert anlegen

Definieren Sie Anwendungsfall, Verantwortlichkeiten und Startpunkt für jeden n8n-Workflow. Versionieren und dokumentieren Sie Änderungen nachvollziehbar.

- Anwendungsfall schriftlich spezifizieren und Ziel dokumentieren.
- Schnittstellen zu Datenquellen, Zielsystemen, Nutzern definieren.
- Verantwortliche für Technik, Organisation und Freigabe benennen.
- Workflows in n8n mit Änderungsverlauf versionieren.

PROCESS

01 Prozessstart dokumentieren
Auslöser und Zielrichtung mit Begründung festhalten.

02 Verantwortliche benennen
Verantwortlichkeiten pro Aufgabe auflisten.

03 Versionierung sichern
Alle Änderungen mit Zeitstempel protokollieren.

MERKSATZ

Eine klare Workflowstruktur schafft dauerhafte Nachvollziehbarkeit und Verlässlichkeit im Betrieb.

MATRIX

2. Datenströme und Schnittstellen gezielt absichern

Sichern Sie alle Datenflüsse in n8n-Workflows gegen unbefugten Zugriff, Datenverlust und Übertragungsfehler.

- Alle Datenflüsse verschlüsseln, Integritätsprüfungen einsetzen.
- Authentifizierung für jede Integration technisch prüfen und dokumentieren.
- Datenarten und Verwendungszweck klassifizieren und transparent machen.

MATRIX

Datenfluss prüfen
Verbindungen regelmäßig technisch überprüfen.

Zugriffsrechte dokumentieren
Rechtevergabe für jedes System dokumentieren.

Prüfpfade anlegen
Systematische Protokollierung automatisieren.

MERKSATZ

Nachvollziehbare Datenwege und begrenzte Zugriffsrechte minimieren Risiken.

TIMELINE

3. Automatisierungsschritte prüfen und Notfallprozeduren einrichten

Implementieren Sie Fehlerkontrolle, Notfallpläne und klare Trennung zwischen manuellen und automatisierten Verarbeitungsschritten.

- Automatisierte von manuellen Prüfungen abgrenzen.
- Fehlerfälle mit Error Nodes und Maßnahmen versehen.
- Notfallkontakte, Eskalationswege und Rückfallebenen dokumentieren.

TIMELINE

- **Fehlerknoten einbauen**
  Jeden Fehlerpfad ausführlich modellieren.
- **Notfallkontakt dokumentieren**
  Kontaktdaten im Workflow hinterlegen.
- **Statusüberwachung aktivieren**
  Automatisierte Statusanzeigen nutzen.

MERKSATZ

Frühzeitige Fehlererkennung und Notfallkonzepte sichern den Betrieb.

CHECKLIST

4. Kontextspezifische Prüfung auf Risiko nach SDM 3.1 D3.2.1

Wenden Sie die SDM-Methode konsequent an: Vorprüfung Art. 35 DSGVO, dann Bewertung nach allen neun EDSA-Kriterien.

1. Pflichten aus Art. 35 Abs. 3 und 4 DSGVO prüfen.
2. Jedes der neun EDSA-Kriterien einzeln dokumentieren.
3. Risiko anhand Anzahl/Tragweite: Zwei Kriterien genügen meist (im Einzelfall auch eins).
4. Kontext berücksichtigen: Datenart, Umfang, Zweck und Umstände bewerten.
5. Keine Punktesysteme einsetzen; nur vollständige Prüfung ist gültig.

MERKSATZ

Sorgfältige Bewertung schafft belastbare und prüfbare Risikoermittlung.

FOCUS

5. Dokumentation, Monitoring und dauerhafte Governance

Halten Sie alle Prüfungen, Anpassungen und Vorfälle revisionssicher fest - für Audit, Aufsicht und eigene Governance-Routinen.

- Regelmäßige Wartungs- und Prüfintervalle schriftlich fixieren.
- Alle Änderungen versioniert aufbewahren.
- Automatisierte, lückenlose Logs und Prüfberichte einrichten.
- Benannte Rollen und Rechte jährlich überprüfen und dokumentieren.

FOCUS

01 Prüfintervalle festlegen
Kontrollzyklen für jede n8n-Instanz planen.

02 Log-Führung sicherstellen
Revisionssichere Speicherung umsetzen.

03 Berechtigungen überwachen
Zugriffsverwaltung jährlich prüfen.

MERKSATZ

Vollständige Dokumentation bildet das Rückgrat einer prüfsicheren Governance.

MATRIX

6. EDSA-Check: Die neun Risikokriterien im Detail (SDM 3.1 D3.2.1)

Hier finden Sie die vollständige Matrix der neun EDSA-Kriterien für eine präzise SDM-Risikoabschätzung.

1 (1) Bewertung/Scoring: Bewertung persönlicher Merkmale.

2 (2) Automatisierte Entscheidung: Rechtswirkung oder signifikante Auswirkung.

3 (3) Überwachung/Tracking: Systematisch, anhaltend, großflächig.

4 (4) Bes. Datenkategorien: Verarbeitung sensibelster Informationen.

5 (5) Umfangreiche Verarbeitung: Viele Betroffene oder hohe Datendichte.

6 (6) Datenzusammenführung: Vernetzung diverses Datenquellen.

7 (7) Schutzbedürftige Gruppen: Kinder, Patienten oder andere besonders betroffene Gruppen.

8 (8) Innovative Methoden: Neuartige technische oder organisatorische Ansätze.

9 (9) Eingriffe in Rechte: Beeinträchtigung von Betroffenenrechten.

MERKSATZ

Nur die vollständige Einzelprüfung schafft eine belastbare SDM-Risikoentscheidung.

MUSTERBEISPIEL

Musterbeispiel: KI-basierte Ticket-Zuordnung via n8n

AUSGANGSLAGE

Service-Abteilung automatisiert die Ticket-Zuordnung: KI analysiert Eingänge und weist sie dem passenden Team zu, manuelle Fehler sollen reduziert werden.

1. Workflow mit definiertem Eingang und Teamrouting-Knoten modellieren.
2. Einsatz von NLP-Logik und Modellen im Workflow dokumentieren.
3. Zugriffsrechte für Ticketdaten und Workflow-Ausgaben prüfen.
4. Vorprüfung nach DSGVO Art. 35 Abs. 3/4 durchführen, EDSA-Kriterien bewerten.
5. Fehler- und Rückfallprozess, z. B. Weiterleitung an Supervisor, abbilden.

ERGEBNIS

Die Ticket-Lösung erfüllt SDM-Governance-Vorgaben. Prüfung und Audit sind für Kontrollstellen nachvollziehbar möglich.

ARBEITSBLATT

Umsetzungscheckliste

- [ ] Anwendungsfall & Ziel dokumentiert?
- [ ] Eingang und Schnittstellen nachvollziehbar modelliert?
- [ ] Verantwortliche und Rollen festgelegt?
- [ ] Sicherheitsmaßnahmen je Integration spezifiziert?
- [ ] Authentifizierung und Rechte geprüft?
- [ ] Automatisierte und manuelle Schritte getrennt?
- [ ] Fehlertoleranz und Backup dokumentiert?
- [ ] Art. 35-Prüfung abgeschlossen?
- [ ] Alle EDSA-Kriterien einzeln geprüft?
- [ ] Kontextuelle Bewertung durchgeführt?
- [ ] Änderungen und Protokolle archiviert?
- [ ] Wartungs- und Prüfroutinen umgesetzt?

Nächster Schritt

Konsequent strukturierte Governance nach SDM in n8n-Workflows sichert Revisionssicherheit und minimiert Kontrollrisiken. Vollständige Anwendung der Prüflogik gewährleistet Nachvollziehbarkeit auch gegenüber externen Prüfinstanzen

WEITERFÜHRENDE ORIENTIERUNG

Gesetzesbibliothek · KI-Risikobibliothek · DAXAIS Academy

www.daxais.de