KI-SICHERHEIT UND KI-GOVERNANCE IM MITTELSTAND · BAND A VON II

Entscheiden und verantworten

Haftung, Regeln, Kosten und Zeit – für alle, die am Ende unterschreiben.

Für Geschäftsführung und Bereichsleitung

55 Seiten

Ausgabe September 2026

Haftung

Normen

Bestandssysteme

Zeitplan

Christian Niebisch · Make Business Intelligent · www.mrpetzai.de

Inhalt
Band A

KI-Sicherheit (DIN, ISO, DSGVO) und KI-Governance im Mittelstand · Vorwort ab Seite 3

1 Die Führungsfrage 5

1.1 Was Sie als Geschäftsführung persönlich verantworten 5

1.2 Die fünf Fragen, an denen jedes KI-Vorhaben geprüft wird 7

1.3 Wer mitreden muss: IT, Betriebsrat, Datenschutz, Fachbereich 9

2 Der Rechtsrahmen in Klartext 11

2.1 DSGVO: die sechs Pflichten, die wirklich greifen 11

2.2 EU-KI-Verordnung: Risikoklassen und was sie bedeuten 14

2.3 Geschäftsgeheimnis, Urheberrecht, Haftung gegenüber Kunden 17

2.4 Mitbestimmung: wann der Betriebsrat zustimmen muss 19

3 Was die Regulierung wirklich kostet 21

3.1 Die ehrliche Rechnung: Aufwand, Zeit, entgangene Geschwindigkeit 21

3.2 Wo die Regel schützt und wo sie nur bremst 23

Inhalt
Band A · Fortsetzung

3.3 Vier Wege, schnell zu bleiben, ohne angreifbar zu werden 25

4 Wo darf die KI laufen? 27

4.1 Eigener Rechner, eigener Server, deutsche Cloud, US-Cloud 27

4.2 Entscheidungstabelle: Jahreskosten, Tempo, Risiko 30

4.3 Der US-Zugriff: CLOUD Act, was er bedeutet, was hilft 32

5 Ihre Bestandssysteme 34

5.1 SAP: warum jede Anbindung über die eigene SAP-Mannschaft läuft 34

5.2 Microsoft Dynamics, Oracle, Infor, DATEV: die kurzen Wege 37

5.3 Was eine Schnittstelle kostet - und was ihre Pflege kostet 39

6 Die KI-Arbeitsrichtlinie 41

6.1 Eine Seite, die Ihre Mitarbeitenden verstehen 41

6.2 Rollen, Freigaben, Vier-Augen-Prinzip 43

Inhalt
Band A · Fortsetzung

6.3	Was bei Verstößen passiert	45
7	**Zeit und Geld**	**46**
7.1	Der realistische Zeitplan: nach 6 Wochen, nach 12 Monaten	46
7.2	Warum Projekte das Dreifache brauchen: die sieben Gründe	48
7.3	Was ein Vorhaben kostet: drei gerechnete Beispiele	50
8	**Der Fragenkatalog an jeden Anbieter**	**52**
9	**Der Notfall: die ersten 24 Stunden**	**54**
A	**Anhang: Richtlinie, Freigabematrix, Prüflisten, Notfallplan**	**55**

Warum dieses Werk zwei Bände hat

Für Geschäftsführung, Bereichsleitung und die IT-Leitung, die am Ende zustimmen muss.

Es gibt zwei Sorten von Büchern über Künstliche Intelligenz. Die einen erzählen, was alles möglich sein wird. Die anderen erklären, was man technisch tun müsste. Beide helfen dem Menschen nicht, der am Ende unterschreibt.

Dieses Werk ist für diesen Menschen geschrieben. Es beantwortet die Fragen, die in Aufsichtsratssitzungen, Betriebsversammlungen und Kundenaudits tatsächlich gestellt werden: Wo liegen unsere Daten? Wer haftet, wenn die Maschine etwas Falsches schreibt? Was dürfen unsere Mitarbeitenden eingeben? Und was kostet uns das, wenn wir es richtig machen?

Warum zwei Bände

Weil zwei Menschen entscheiden müssen und beide etwas anderes brauchen. Die Geschäftsführung braucht Klarheit über Verantwortung, Geld und Zeit. Die IT-Leitung braucht Architekturen, Schnittstellen und Prüfpläne. Wird beides in ein Buch gezwängt, liest es keiner von beiden zu Ende.

Die IT ist dabei nicht die ausführende Abteilung, sondern die entscheidende. Wenn die IT-Leitung sagt, das sei zu unsicher oder so stimme das nicht, ist jedes KI-Vorhaben beendet - und zwar zu Recht, denn sie kennt die Altlasten, die Berechtigungen und die Verträge. Deshalb ist Band B kein Anhang, sondern ein eigenständiges Werk, und deshalb steht in ihm keine Aussage, die nicht an einem laufenden System aufgebaut, gemessen und wieder auseinandergenommen wurde.

Ihre Systeme, Ihre Kosten

SAP, Dynamics, DATEV – und warum das eigene Kapitel dazu im Technikband steht.

Die Systeme, die Sie schon haben

Kein mittelständisches Haus fängt bei null an. In den meisten großen Betrieben steht SAP im Zentrum: S/4HANA oder noch ECC, dazu Microsoft Dynamics, Oracle, Infor oder Sage, in der Buchhaltung häufig DATEV, im Vertrieb Salesforce oder HubSpot. Jede KI, die wirklich Arbeit abnehmen soll, muss an diese Systeme heran - und genau dort entstehen die Kosten, die kein Anbieter auf seine erste Folie schreibt.

Deshalb hat SAP in diesem Werk ein eigenes Kapitel. Nicht, weil die Anbindung unmöglich wäre - OData, BAPI, RFC und die Dienste der BTP sind dokumentiert und belastbar -, sondern weil sie ein Projekt mit Ihrer eigenen SAP-Mannschaft ist, mit Berechtigungen, Testmandant, Abnahme und Pflege nach jedem Update. Wer das vorher weiß, plant richtig. Wer es hinterher erfährt, hat ein Projekt, das dreimal so lange dauert wie geplant.

Was dieses Werk nicht ist

Es ist keine Rechtsberatung und keine Zertifizierung. Es nennt keine Zahl ohne Quelle und verspricht keine Prozente. Wo etwas offen ist, steht das da. Was Sie hier bekommen, sind Entscheidungsgrundlagen, Musterdokumente zum Übernehmen und Prüflisten, mit denen Sie jeden Anbieter - mich eingeschlossen - an derselben Latte messen können.

Christian Niebisch

Hundsangen, September 2026

KI-SICHERHEIT UND KI-GOVERNANCE IM MITTELSTAND · BAND B VON II

Bauen
und betreiben

Architekturen, Schnittstellen, Modelle, Prüfpläne –
jede Angabe an einem laufenden System gemessen.

Für IT-Leitung und Administration · 96 Seiten · Ausgabe September 2026

Architektur · SAP · Schnittstellen · Abnahme

Christian Niebisch · Make Business Intelligent · www.mrpetzai.de

Inhalt
Band B

Architektur, Schnittstellen und Prüfpläne für die IT-Leitung

1	**Drei Referenzarchitekturen**	**5**
1.1	Einzelrechner im Haus: Aufbau, Grenzen, Kosten	5
1.2	Server im eigenen Rechenzentrum	10
1.3	Deutsche Cloud: was der Vertrag hergibt	15
1.4	Datenflüsse, Zonen, Ports: drei Zeichnungen zum Nachbauen	20
2	**Identitäten, Schlüssel, Rechte**	**24**
2.1	Wo API-Schlüssel liegen dürfen und wo nicht	24
2.2	Schlüsselwechsel im laufenden Betrieb	27
2.3	Das Prinzip der kleinsten Rechte in der Praxis	29
3	**Transport und Speicher**	**32**
3.1	TLS, Zertifikate, was ein Proxy sieht	32
3.2	Verschlüsselung, Sicherung, Wiederanlauf	35

Inhalt
Band B · Fortsetzung

3.3 Löschfristen technisch durchgesetzt 38

4 Ablaufsteuerung: n8n, Make, Zapier 40

4.1 Webhooks absichern: Signatur statt geratener Adresse 40

4.2 Zugangsdaten: Verschlüsselung, Trennung Test und Betrieb 43

4.3 Ausführungsprotokolle: welche Kundendaten dort landen 46

4.4 Aktualisierungen ohne Ausfall 49

5 CRM- und Fremdsysteme 51

5.1 HubSpot: Zugriffstoken, Rechteumfang, Ratengrenzen 51

5.2 Salesforce: Verbundene App, Feldrechte, Protokoll 54

5.3 Pipedrive und andere: das gleiche Prüfschema 57

5.4 Datenminimierung und Löschweitergabe 59

Inhalt
Band B · Fortsetzung

6	**SAP anbinden**	**61**
6.1	Die drei Wege: OData über den Gateway, BAPI und RFC, SAP BTP	61
6.2	Berechtigungen, Mandanten, Testsystem: wer was freigibt	65
6.3	S/4HANA, ECC und Cloud-Editionen: was sich unterscheidet	68
6.4	Nach dem nächsten Update: Pflege, Abnahme, Zuständigkeit	71
6.5	Kosten und Dauer, ehrlich gerechnet	73
7	**Sprachmodelle anbinden**	**75**
7.1	Fremdes Modell: was hinausgeht, was gespeichert wird	75
7.2	Lokales Modell: Hardware, Durchsatz, Kosten je Vorgang	78
7.3	Die Trennlinie: welche Datenart in welches Modell darf	82

Inhalt
Band B · Fortsetzung

8	**Angriffe auf KI-Systeme**	**84**
8.1	Prompt-Injection über Webseiten, Mails und Anhänge	84
8.2	Datenabfluss über Protokolle und Zwischenspeicher	87
8.3	Manipulierte Quellen und vergiftete Wissensbestände	89
8.4	Je Angriff die Gegenmaßnahme und der Test dazu	91
9	**Betrieb und Abnahme**	**93**
9.1	Protokollierung, Alarme, Patchstand	93
9.2	Der Prüfplan zum Abhaken für die IT-Leitung	95
B	**Anhang: Konfigurationen, Prüfplan, Betriebshandbuch**	**96**

KI-Arbeitsrichtlinie der ‹Firma›

Muster zum Übernehmen · beschlossen von der Geschäftsführung · gilt für alle Mitarbeitenden

1 · Wozu diese Richtlinie

KI-Werkzeuge helfen uns, schneller zu arbeiten. Sie nehmen uns die Verantwortung nicht ab. Diese Seite sagt, was erlaubt ist, was nicht und wer entscheidet.

2 · Erlaubte Werkzeuge

WERKZEUG	FREIGEGEBEN FÜR	NICHT ERLAUBT FÜR
<lokales Modell>	alle Texte, auch mit Kundenbezug	–
<Cloud-Dienst>	Recherche, Entwürfe ohne Personenbezug	Kunden- und Personaldaten, Angebote
private Konten	–	jede dienstliche Nutzung

3 · Was nie eingegeben wird

- Namen, Adressen, Telefonnummern und Mailadressen von Kunden, Bewerbern, Mitarbeitenden
- Gesundheits-, Personal- und Gehaltsdaten
- Preise, Kalkulationen, Verträge, Konstruktionsdaten
- Zugangsdaten, Kennwörter, Schlüssel
- alles, was Sie einem Wettbewerber nicht zeigen würden

> **Im Zweifel gilt**
>
> Erst fragen, dann eingeben. Alles, was das Haus verlässt, wird von einem Menschen gelesen und freigegeben: Die KI schlägt vor, der Mensch entscheidet und unterschreibt.

Hier endet die Leseprobe.

Die beiden Bände sind nicht öffentlich. Wenn Sie hineinsehen möchten, vereinbaren wir einen kostenlosen Kennlerntermin – dreißig Minuten über Teams, zu einem Termin Ihrer Wahl.

Ich zeige Ihnen darin, wie die Antworten aus diesen beiden Bänden an einem laufenden System aussehen: wo die Daten liegen, wer haftet, was die Mitarbeitenden dürfen und was eine belastbare Antwort darauf kostet. Sie sagen mir, wo es bei Ihnen klemmt – und bekommen eine ehrliche Einschätzung, ob sich der Aufwand für Sie lohnt.

Der nächste Schritt

Schlagen Sie einfach drei Termine vor, abends geht auch.

Kennlerntermin vereinbaren

Christian Niebisch · Mr.PetzAI · Hauptstr. 50 · 56414 Hundsangen
christian.niebisch@mrpetzai.de · 015562 / 511 169 · www.mrpetzai.de