DATENSCHUTZEXPERTE24.NET

KOSTENLOSE CHECKLISTE

Welche KI-Use-Cases sind für Sie DSGVO-sicher?

Bevor Sie Zeit und Geld investieren: Die Checkliste zeigt, welche KI-Anwendungsfälle sich lohnen — und worauf Sie beim Datenschutz achten müssen.

- Die häufigsten KI-Use-Cases nach Abteilung
- DSGVO-Ampel je Use-Case: grün · gelb · rot
- Selbst entwickeln vs. Dienstleister: die richtigen Fragen

Karl Pusch · Zertifizierter Datenschutzbeauftragter (TÜV Rheinland) · ISO 27701

Stand: Juli 2026
BOP BLUEOCEAN PRIVACY LTD

SO LESEN SIE DIE CHECKLISTE

Die Ampel bewertet nicht die Technik. Sie bewertet den Einsatz.

Derselbe KI-Dienst kann grün oder rot sein — je nachdem, welche Daten hineingehen und was mit dem Ergebnis passiert. Die Ampel bewertet den Use-Case, nicht das Werkzeug.

GRÜN

Kein Personenbezug oder klar tragfähige Rechtsgrundlage. Ergebnis wird von Menschen genutzt, nicht automatisch vollzogen. Start ohne größeren Vorlauf möglich.

GELB

Personenbezug vorhanden, aber gestaltbar. Braucht Auftragsverarbeitung, Zweckbindung, Löschkonzept — teils eine Datenschutz-Folgenabschätzung.

ROT

Verboten, hochrisikoreich oder rechtlich sehr eng. Nicht ohne vorherige Prüfung starten. Manche dieser Fälle sind seit 02.02.2025 untersagt.

Vier Fragen, die jede Farbe bestimmen

- **1 · Sind personenbezogene Daten im Spiel?**
  Auch indirekt: IP-Adressen, Kundennummern, Freitextfelder, Meeting-Teilnehmer, Bewerbungsunterlagen. Ein „anonymer" Prompt ist selten anonym.
- **2 · Wird die Ausgabe automatisch vollzogen?**
  Art. 22 DSGVO greift, wenn eine Entscheidung mit rechtlicher Wirkung ohne menschliches Zutun fällt. Ein Mensch, der nur abnickt, genügt nicht.
- **3 · Wo werden die Daten verarbeitet?**
  Drittlandtransfer braucht Angemessenheitsbeschluss oder geeignete Garantien plus Transfer-Folgenabschätzung. Ein Häkchen im Anbieterportal ersetzt das nicht.
- **4 · Betrifft es Beschäftigte oder besondere Datenkategorien?**
  Gesundheit, Herkunft, Gewerkschaft, Biometrie (Art. 9 DSGVO) und Beschäftigtenkontexte verschieben die Ampel fast immer nach rot.

Die eine Regel, die alle Farben überschreibt. Wer personenbezogene Daten in einen KI-Dienst gibt, für den kein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO vorliegt, verarbeitet ohne Rechtsgrundlage. Der kostenlose Consumer-Zugang eines KI-Anbieters ist in aller Regel kein Auftragsverarbeitungsverhältnis.

Aus grün wird rot — durch die Wahl des Zugangs, nicht durch den Use-Case.

USE-CASES NACH ABTEILUNG · TEIL 1

Marketing, Vertrieb, Kundenservice

Marketing & Vertrieb

●	**Textentwürfe, Bildideen, Rechercheaufbereitung ohne Kundendaten** Keine personenbezogenen Daten im Prompt. Urheber- und Geschäftsgeheimnisfragen bleiben davon unberührt.	GRÜN
●	**E-Mail-Personalisierung aus CRM-Daten** Personenbezug. Braucht AVV, Zweckbindung, Informationspflicht nach Art. 13. Kein Training auf Ihren Daten — vertraglich ausschließen.	GELB
●	**Lead-Scoring als Entscheidungshilfe für den Vertrieb** Zulässig gestaltbar, solange ein Mensch entscheidet und den Score überstimmen kann. Dokumentieren, dass er es tatsächlich tut.	GELB
●	**Automatische Ablehnung oder Konditionsvergabe per Score** Automatisierte Einzelentscheidung mit erheblicher Wirkung — Art. 22 DSGVO. Nur in engen Ausnahmen und mit Schutzmaßnahmen.	ROT

Kundenservice

●	**FAQ-Chatbot auf eigener Wissensdatenbank, ohne Kontodaten** Grün im Datenschutz. Ab 02.08.2026 gilt zusätzlich die Transparenzpflicht nach Art. 50 KI-VO: Nutzer müssen erkennen, dass sie mit einer KI sprechen.	GRÜN
●	**Ticket-Kategorisierung und Antwortvorschläge** Personenbezug im Ticketinhalt. Freitextfelder enthalten regelmäßig mehr, als das Formular vorsieht — auch Gesundheitsdaten.	GELB
●	**Gesprächszusammenfassung aus Telefonaten** Aufzeichnung braucht eigene Rechtsgrundlage und Hinweis. Zusammenfassen einer rechtmäßig erhobenen Aufzeichnung ist gestaltbar.	GELB
●	**Emotionserkennung in Stimme oder Gesicht von Beschäftigten** Am Arbeitsplatz nach Art. 5 KI-VO untersagt. Das Verbot gilt seit 02.02.2025. Nicht durch Betriebsvereinbarung heilbar.	ROT

Das häufigste Missverständnis. „Wir geben ja keine Namen ein." Ein Support-Ticket ohne Namen, aber mit Kundennummer, Vertragsdetail und Beschwerdegrund ist personenbezogen. Pseudonymisierung ist keine Anonymisierung — sie senkt das Risiko, sie beendet nicht die Anwendbarkeit der DSGVO.

USE-CASES NACH ABTEILUNG · TEIL 2

Personal, Finanzen, IT

Personal & Recruiting

Stellenanzeigen formulieren, Onboarding-Texte, interne Leitfäden — GRÜN

Kein Personenbezug. Prüfen Sie das Ergebnis auf diskriminierende Formulierungen — die Verantwortung bleibt bei Ihnen.

Zusammenfassung von Bewerbungsgesprächen für das Protokoll — GELB

Personenbezug, Bewerberkontext. Braucht AVV, kurze Speicherfrist, Information der Bewerber. Keine Bewertung durch die KI.

Vorsortierung oder Rangfolge von Bewerbungen — ROT

Nach Anhang III KI-VO als Hochrisiko eingestuft. Zusätzlich Art. 22 DSGVO, wenn die Sortierung faktisch aussiebt.

Stress-, Aufmerksamkeits- oder Emotionsanalyse von Mitarbeitenden — ROT

Verbot nach Art. 5 KI-VO, gilt seit 02.02.2025. Unabhängig von Einwilligung.

Finanzen & Buchhaltung

Berichtstexte aus aggregierten Kennzahlen — GRÜN

Sofern die Aggregation keinen Rückschluss auf Einzelpersonen erlaubt — bei kleinen Einheiten kritisch prüfen.

Belegerkennung und Kontierungsvorschläge — GELB

Belege enthalten Namen, Bankdaten, teils Gesundheitsbezug (Arztrechnungen). AVV und Verarbeitungsort klären.

Bonitätsbewertung natürlicher Personen — ROT

Hochrisiko nach Anhang III KI-VO. Zusätzlich Art. 22 DSGVO, wenn automatisch über Vertrag oder Konditionen entschieden wird.

IT & Entwicklung

Code-Assistenz auf eigenem Code ohne Produktivdaten — GRÜN

Datenschutzrechtlich unkritisch. Geschäftsgeheimnisse und Lizenzkonformität des Ergebnisses sind eigene Themen.

Log-Analyse und Anomalieerkennung — GELB

IP-Adressen sind personenbezogene Daten. Wenn Logs Mitarbeitendenaktivität abbilden, kommt Verhaltenskontrolle hinzu.

Produktivdaten als Testdaten für KI-Features — GELB

Häufigster Fehler in der Entwicklung. Zweckänderung, meist ohne Rechtsgrundlage. Synthetische Daten oder echte Anonymisierung.

Biometrische Fernidentifizierung in öffentlich zugänglichen Räumen — ROT

Nach Art. 5 KI-VO grundsätzlich untersagt, mit engen Ausnahmen für Strafverfolgungsbehörden. Für Unternehmen: nein.

DIE ROLLENFRAGE

Selbst entwickeln oder Dienstleister?

Die Entscheidung ist keine Kostenfrage. Sie entscheidet, welche Rolle Sie nach der KI-Verordnung einnehmen — und damit, welche Pflichten Sie treffen.

Art. 25 KI-VO, der Satz, den kaum jemand gelesen hat. Wer ein KI-System unter eigenem Namen oder eigener Marke in Verkehr bringt oder es wesentlich verändert, gilt selbst als **Anbieter** — nicht mehr als Betreiber.

Praktisch: Ein zugekauftes Modell mit eigenem Logo, eingebettet in Ihr Produkt und an Kunden ausgeliefert, kann Sie zum Anbieter machen. Anbieter tragen deutlich weitergehende Pflichten als Betreiber. Die Einordnung ist eine Einzelfallprüfung, kein Automatismus.

Selbst entwickeln

- Volle Kontrolle über Daten und Verarbeitungsort
- Keine Subprozessorenkette, kein Drittlandtransfer
- Aber: Sie sind sehr wahrscheinlich Anbieter nach Art. 25
- Sie tragen Dokumentation, Risikomanagement, Konformität
- Bei Hochrisiko-Anwendungen erheblicher Aufwand
- Sinnvoll bei sensiblen Daten und dauerhaftem Kernprozess

Dienstleister nutzen

- Schneller Start, geringere Anfangskosten
- Anbieterpflichten bleiben beim Anbieter — solange Sie nichts wesentlich verändern
- Aber: AVV, Subprozessoren, Verarbeitungsort werden Ihr Thema
- Betreiberpflichten treffen Sie trotzdem (u. a. Art. 4 KI-Kompetenz)
- Abhängigkeit von Modellwechseln und Preisänderungen
- Sinnvoll bei Standardaufgaben ohne Alleinstellung

Sechs Fragen an jeden KI-Dienstleister — vor der Unterschrift

01 **Liegt ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO vor?**
Mit vollständiger Liste der Subprozessoren und Informationspflicht bei Änderung. **Kein AVV = kein Personenbezug hineingeben.**

02 **Wo werden die Daten verarbeitet und gespeichert?**
Region konkret benennen lassen, nicht „EU-Rechenzentren verfügbar". Bei Drittlandbezug: Angemessenheitsbeschluss oder Garantien plus Transfer-Folgenabschätzung.

03 **Werden unsere Eingaben zum Training verwendet?**
Vertraglich ausschließen, nicht per Einstellung im Portal. Einstellungen ändern sich mit dem nächsten Release. **Verträge nicht.**

04 **Sind Sie Anbieter nach KI-VO — und was sind dann wir?**
Lassen Sie sich die Rollenzuordnung schriftlich geben. Wer die Frage nicht beantworten kann, hat sie sich nicht gestellt.

05 **Wie lange werden Prompts und Ausgaben gespeichert?**
Retention-Zeitraum, Löschprozess, Ausnahmen für „Missbrauchserkennung". Letztere ist oft der Punkt, an dem die versprochene Löschung nicht stattfindet.

06 **Was passiert bei Modellwechsel oder Vertragsende?**
Exportierbarkeit, Rückgabe, Löschnachweis. Und: Ändert ein Modellwechsel das Ergebnis so, dass Ihre Dokumentation nicht mehr stimmt?

FRISTEN & STARTCHECK

Was schon gilt — und was kommt

02.02.2025
Art. 5 KI-VO — Verbote
Verbotene Praktiken gelten. Darunter Emotionserkennung am Arbeitsplatz und biometrische Fernidentifizierung in öffentlich zugänglichen Räumen.

02.02.2025
Art. 4 KI-VO — KI-Kompetenz
Anbieter und Betreiber müssen für ausreichende KI-Kompetenz ihres Personals sorgen. Betrifft praktisch jedes Unternehmen, das KI einsetzt.

02.08.2026
Art. 50 KI-VO — Transparenz
Kennzeichnungspflichten. Nutzer müssen erkennen, dass sie mit einer KI interagieren; bestimmte KI-Inhalte sind zu kennzeichnen.

Zum Digital Omnibus. Auf EU-Ebene wird über Anpassungen an Fristen und Pflichten der KI-Verordnung beraten. Das Verfahren ist zum Redaktionsschluss dieser Checkliste nicht abgeschlossen. Planen Sie mit den geltenden Daten — und prüfen Sie den Verfahrensstand, bevor Sie Fristen intern kommunizieren.

Startcheck — zehn Punkte vor dem ersten Use-Case

- [ ] Use-Case beschrieben: Welche Daten gehen hinein, was passiert mit dem Ergebnis?
  Ein Satz. Wer ihn nicht schreiben kann, hat keinen Use-Case, sondern ein Werkzeug.
- [ ] Personenbezug geprüft — auch in Freitextfeldern, Anhängen und Logs.
- [ ] Rechtsgrundlage bestimmt und dokumentiert (Art. 6, ggf. Art. 9 DSGVO).
- [ ] Auftragsverarbeitungsvertrag mit dem KI-Anbieter liegt vor, Subprozessoren bekannt.
- [ ] Verarbeitungsort geklärt; bei Drittlandbezug Garantien und Transfer-Folgenabschätzung.
- [ ] Training auf eigenen Daten vertraglich ausgeschlossen.
- [ ] Verzeichnis von Verarbeitungstätigkeiten ergänzt (Art. 30 DSGVO).
- [ ] Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist (Art. 35 DSGVO).
- [ ] Rolle nach KI-VO bestimmt: Anbieter oder Betreiber — schriftlich, mit Begründung.
- [ ] KI-Kompetenz nach Art. 4 KI-VO: Schulung durchgeführt, Teilnahme nachweisbar.

Wenn Sie neun von zehn Haken setzen können, ist der Use-Case startklar. Fehlt der AVV oder die Rollenzuordnung, fehlt nicht ein Haken — dann fehlt die Grundlage.

NÄCHSTER SCHRITT

Eine Checkliste ersetzt keine Prüfung Ihres Falls.

Sie zeigt Ihnen, welche Fragen zu stellen sind. Welche Antwort für Ihr Unternehmen gilt, hängt an Ihren Daten, Ihren Verträgen und Ihrer Rolle nach der KI-Verordnung.

Beratungsgespräch buchen

45 Minuten, feste Kosten, kein Abo. Wir gehen Ihre konkreten Use-Cases durch, ordnen die Rolle nach KI-Verordnung ein und benennen die Punkte, die vor dem Start geklärt sein müssen.

datenschutzexperte24.net/termin/

Karl Pusch · Zertifizierter Datenschutzbeauftragter (TÜV Rheinland) · ISO 27701 · über sechs Jahre Praxis im Datenschutz

Was Sie mitbringen sollten. Eine Liste der KI-Dienste, die in Ihrem Haus bereits genutzt werden — auch die, die niemand freigegeben hat. In den meisten Erstgesprächen ist diese Liste länger als erwartet.

Herausgeber: BOP BLUEOCEAN PRIVACY LTD · HE 464125 · Delphon 8, Livadia Office 204, 7060 Larnaca, Zypern · VAT CY60114734R · datenschutzexperte24.net