ANHANG E

DSGVO-Checklisten

Zusatzmaterial zum Buch „PREDICTABLE“ von Thorsten Pätzold — Amazing Agents.

ANHANG E

DSGVO-Checklisten

Praxis-Werkzeuge für die rechtskonforme Agent-Einführung

Dieser Anhang ist keine Rechtsberatung. Er ist eine strukturierte Sammlung der Punkte, die in unseren Projekten regelmäßig geprüft werden müssen. Konkrete Rechtsfragen klären Sie mit einem Datenschutzanwalt — diese Checklisten helfen Ihnen, das Gespräch effizient zu führen.

„DSGVO ist kein Hindernis. Sie ist eine Architektur-Anforderung. Wer sie ab Tag 1 mitdenkt, baut robuste Systeme.“

E.1 Pre-Setup-Check (vor Start eines Agent-Projekts)

Diese 18 Punkte werden vor jeder Setup-Phase durchgegangen. Wenn auch nur einer offen ist, startet das Projekt nicht.

Nr.	Prüfpunkt	Antwort	Verantwortlich
1	Verzeichnis von Verarbeitungstätigkeiten existiert	ja/nein	DSB
2	Datenschutz-Folgenabschätzung erforderlich?	ja/nein	DSB
3	Rechtsgrundlage definiert (Art. 6 DSGVO)	ja/nein	Recht
4	Personenbezogene Daten identifiziert	ja/nein	Fach
5	Sensible Daten (Art. 9) ausgeschlossen	ja/nein	Fach
6	Zweck der Verarbeitung dokumentiert	ja/nein	Fach
7	Datenminimierungs-Prinzip geprüft	ja/nein	Fach
8	Speicherdauer / Löschfristen definiert	ja/nein	DSB
9	AVV mit Modell-Anbieter geschlossen	ja/nein	Recht
10	EU- oder US-Hosting?	EU/US	IT
11	Bei US-Hosting: SCC + TIA durchgeführt	ja/nein	Recht
12	TOM-Konzept dokumentiert	ja/nein	IT
13	Zugriffs-Konzept (Need-to-know)	ja/nein	IT
14	Audit-Logging aktiviert	ja/nein	IT
15	Datenschutz-Hinweise auf Webseite ergänzt	ja/nein	Marketing
16	Beschäftigte informiert (Art. 13)	ja/nein	HR
17	Betriebsrat eingebunden	ja/nein	HR
18	Notfallplan bei Datenpanne	ja/nein	DSB

> ***LESART DER TABELLE*** *DSB = Datenschutzbeauftragter, IT = IT-Verantwortlicher, Recht = Rechtsabteilung oder externer Anwalt, Fach = Fachbereich, der den Agenten einsetzt. Wenn eine Spalte „Verantwortlich“ keine eindeutige Person hat, ist das Projekt nicht startbereit. Verantwortung muss benannt sein.*

E.2 Datenfluss-Inventar

Welche Daten gehen wohin? Diese Vorlage ist die Pflicht-Übung in jedem Projekt. Sie ist die Grundlage für AVV, TOM, und Datenschutz-Folgenabschätzung.

Daten-Typ	Quelle	Empfänger	Zweck	Rechtsgrundlage	Speicherdauer
Mail-Inhalt	Outlook	OpenAI EU	Klassifizierung	Art. 6 (1) f	0 Tage (kein Speichern)
Lead-Profil	CRM	Modell-Anbieter	Outreach	Art. 6 (1) f	12 Monate
Bewerber-CV	Bewerbungs-Tool	Modell-Anbieter	Sichtung	Art. 6 (1) b	6 Monate nach Verfahren
Vertragsdaten	DMS	Modell-Anbieter	Extraktion	Art. 6 (1) b	Vertragsdauer + 10 J.
Ticket-Inhalt	Helpdesk	Modell-Anbieter	Antwort-Entwurf	Art. 6 (1) b	3 Jahre
Kunden-Mail-Adresse	CRM	Mail-Server	Versand	Art. 6 (1) b	Bis Widerspruch

Diese Tabelle wird als Anlage zum Verzeichnis der Verarbeitungstätigkeiten geführt. Bei jeder Änderung — neuer Datenfluss, anderer Anbieter, anderer Zweck — wird sie aktualisiert. Der DSB sollte sie quartalsweise reviewen.

E.3 AVV — Mindest-Inhalte für Modell-Anbieter

Jeder Auftragsverarbeitungs-Vertrag mit einem Modell-Anbieter (OpenAI, Anthropic, Google, Microsoft, etc.) muss folgende Punkte abdecken. Wenn einer fehlt, ist der AVV unvollständig.

- *Gegenstand und Dauer der Auftragsverarbeitung — was wird wann verarbeitet?*
- *Art und Zweck der Verarbeitung — wofür werden die Daten genutzt?*

- *Art der personenbezogenen Daten und Kategorien betroffener Personen — wer ist betroffen, welche Daten?*
- *Pflichten und Rechte des Verantwortlichen — was darf der Auftraggeber kontrollieren?*
- *Weisungsgebundenheit des Auftragsverarbeiters — keine Eigeninitiative beim Anbieter*
- *Vertraulichkeitsverpflichtung der Mitarbeiter beim Anbieter*
- *Technische und organisatorische Maßnahmen — TOM-Konzept als Anlage*
- *Unterauftragsverhältnisse — welche Sub-Anbieter werden eingesetzt? Genehmigungspflicht?*
- *Unterstützung bei Betroffenenrechten — wie schnell muss der Anbieter bei Auskunfts-Anfragen reagieren?*
- *Meldepflichten bei Datenpannen — Frist (max. 72 Stunden Richtung Behörde, vom Anbieter typisch 24-48 Stunden Richtung Auftraggeber)*
- *Datenrückgabe und Löschung nach Vertragsende — wie und wann?*
- *Audit-Rechte — wie und in welchem Umfang darf der Auftraggeber prüfen?*

PRAXIS-TIPP *Jeder seriöse Modell-Anbieter stellt eine AVV-Vorlage. Lesen Sie sie nicht nur — vergleichen Sie mit dieser Liste. Lücken sind Anlass für Nachverhandlung. Wenn der Anbieter nicht*

> *verhandelt: anderer Anbieter.*

E.4 Betroffenen-Rechte: Eskalations-Pfade

Wenn ein Kunde Auskunft, Löschung oder Übertragung verlangt, muss Ihr Agent-Setup darauf vorbereitet sein. Diese Tabelle zeigt die typischen Anfragen und die Pfade durch Ihr System.

Anfrage	Frist	Was zu prüfen	Was zu tun
Auskunft (Art. 15)	1 Monat	Welche Daten zur Person liegen vor?	Vollständige Liste aus allen Systemen, inkl. Memory-Layer der Agenten
Berichtigung (Art. 16)	1 Monat	Welche Datenpunkte sind betroffen?	Korrektur in allen Systemen, inkl. Vector-Stores
Löschung (Art. 17)	1 Monat	Bestehen Aufbewahrungspflichten?	Wo Aufbewahrung pflichtig: Sperren statt Löschen. Sonst: vollständige Löschung.
Einschränkung (Art. 18)	1 Monat	Was bleibt aus Verarbeitung	Markierung in allen Systemen, Verarbeitungs-Stopp im Agent
Datenübertragbarkeit (Art. 20)	1 Monat	Welche Daten waren Eingabe der Person?	Strukturiertes Format (JSON, CSV) bereitstellen
Widerspruch (Art. 21)	Sofort	Direkt-Marketing? Sofort stoppen.	Kunde aus allen Outreach-Listen entfernen, Memory-Eintrag setzen

Die kürzeste Frist ist Sofort — bei Widerspruch gegen Direktmarketing. Ihr Outreach-Agent muss eine Stop-Liste im Memory haben, die binnen Stunden wirkt. Wer 14 Tage später noch Mails sendet, hat ein Compliance-Problem.

E.5 Datenschutz-Folgenabschätzung — Template

Eine DSFA ist nötig, wenn die Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat“. Bei Agent-Projekten ist das oft der Fall — insbesondere bei automatisierter Entscheidungsfindung, großem Datenumfang oder neuen Technologien.

Pflicht-Felder einer DSFA

- *Systematische Beschreibung der geplanten Verarbeitung — was passiert wann mit welchen Daten?*
- *Bewertung der Erforderlichkeit und Verhältnismäßigkeit — geht es nicht datensparsamer?*
- *Risikobewertung — welche Risiken bestehen für die Betroffenen?*
- *Geplante Abhilfemaßnahmen — wie werden Risiken minimiert?*
- *Konsultation des Datenschutzbeauftragten — schriftliche Stellungnahme*
- *Einbindung der Aufsichtsbehörde, wenn Restrisiken trotz Maßnahmen hoch bleiben*

Typische Risiken bei Agent-Projekten

- *Halluzinationen führen zu falschen Aussagen über Personen — Reputations-Schaden*
- *Memory-Layer enthält Personen-Daten, die schwer löschbar sind*
- *Prompt Injection führt zu unbeabsichtigter Daten-Weitergabe*
- *Modell-Drift führt zu Diskriminierung trotz neutraler Prompts*

- *Tool-Zugriffe gehen über das Need-to-know hinaus*

Typische Abhilfemaßnahmen

- *Mensch-in-the-Loop bei externer Kommunikation*
- *Pseudonymisierung im Memory-Layer*
- *Trennung von Daten und Anweisungen (Prompt-Injection-Schutz)*
- *Quartalsweise Bias-Audits gegen geschützte Merkmale*
- *Need-to-know-Zugriffsmodell mit minimalen Tool-Berechtigungen*
- *Vollständige Audit-Logs mit 12-Monaten-Aufbewahrung*
- *Klare Eskalations-Trigger für sensible Themen*

E.6 Notfallplan bei Datenpanne

Wenn etwas schiefgeht, zählt nicht die Frage „warum“. Es zählt die Frage „was als nächstes“. Diese Reihenfolge muss vor dem ersten Tag in Produktion stehen.

Stunde	Was zu tun	Wer
0–1	Vorfall feststellen, dokumentieren	Erkenner + IT
1–2	Agent stoppen, Schaden begrenzen	IT
2–4	Forensik starten: was ist passiert?	IT + DSB
4–8	Betroffene Personen identifizieren	DSB
8–24	Interne Meldung an Geschäftsleitung	DSB
24–48	Externe Bewertung: Meldepflicht ggü. Behörde?	DSB + Recht
48–72	Wenn ja: Meldung an Aufsichtsbehörde (Pflicht!)	DSB
72–168	Kommunikation an Betroffene, wenn hoch riskant	DSB + Comms
danach	Lessons Learned, Prozess-Anpassung	alle

> ***72-STUNDEN-REGEL*** *Ab Kenntnis einer meldepflichtigen Datenpanne haben Sie 72 Stunden Zeit, sie der Aufsichtsbehörde zu melden. Diese 72 Stunden laufen — auch am Wochenende, auch in Urlaubszeiten. Ein klarer Notfallplan mit Vertretungs-Regelungen ist Pflicht.*

E.7 Anti-Diskriminierungs-Checkliste (besonders für Recruiting)

Das AGG schützt vor Diskriminierung wegen Alter, Geschlecht, Herkunft, Religion, Behinderung, sexueller Identität und Weltanschauung. Agent-Setups, die Personen-Daten verarbeiten und Entscheidungen vorbereiten, müssen diese Risiken aktiv adressieren.

- *Werden geschützte Merkmale aus Eingangs-Daten entfernt, bevor das Modell sie sieht? (Foto entfernen, Geburtsdatum maskieren, Namen ggf. anonymisieren)*
- *Werden Proxies für geschützte Merkmale erkannt und ausgeschlossen? (Postleitzahl als Proxy für Herkunft, Hobbies als Proxy für Alter)*

- *Werden die Output-Ergebnisse quartalsweise auf Disparität geprüft? (Werden Bewerberinnen genauso oft eingeladen wie Bewerber bei vergleichbarem Profil?)*
- *Existiert ein menschlicher Override-Punkt vor der finalen Entscheidung?*
- *Sind Begründungen für Absagen so formuliert, dass sie nicht auf geschützten Merkmalen basieren?*
- *Wird dokumentiert, welcher Prompt mit welcher Modell-Version welche Entscheidung beeinflusst hat? (Audit-Trail bei Klagen)*
- *Hat ein Bewerber das Recht, eine menschliche Überprüfung zu verlangen — und wie wird dieses Recht kommuniziert?*

„Ein Agent, der Diskriminierungs-Risiken nicht aktiv reduziert, ist nicht ein neutraler Helfer. Er ist ein Multiplikator existierender Vorurteile in den Trainingsdaten."

> ***MINDEST-PRAXIS*** *Quartalsweise Disparitäts-Audits. Vergleich der Outputs gegen demografische Anteile in der Bewerbungs-Population. Bei signifikanten Abweichungen: Prompt-Anpassung, Trainings-Daten-Review, ggf. Modell-Wechsel. Diese Audits werden dokumentiert und sind Bestandteil der Compliance-Akte.*

E.8 Letzter Punkt: Realitätscheck

DSGVO ist keine Tugend, die Sie in einer ruhigen Stunde erwerben können. Sie ist eine kontinuierliche Praxis. Die meisten Mittelständler unterschätzen, wie sehr Agent-Setups die Aufmerksamkeit auf Datenschutz erhöhen — Aufsichtsbehörden bekommen mehr Beschwerden, Konkurrenten beobachten genauer, Mitarbeiter stellen mehr Fragen.

Wer DSGVO-Themen als Bremsklotz behandelt, verzögert sich selbst. Wer sie als Architektur-Anforderung behandelt, baut Setups, die zehn Jahre tragen — auch wenn sich Modelle, Anbieter und Tools ändern. Die Datenschutz-Grundlagen ändern sich nicht. Die Gestaltung eines konformen Setups ist eine einmalige

Investition mit dauerhafter Rendite.

„Wer DSGVO als Pflicht erlebt, hat sie zu spät verstanden. Wer sie als Architektur erlebt, baut robust.“

Dieses Dokument ist Anhang E zum Buch „PREDICTABLE — Wie KI-Agenten Ihr Business von Spielzeug zu Infrastruktur transformieren“ (Thorsten Pätzold, Amazing Agents, Pirmasens 2026). Verweise auf Kapitel beziehen sich auf das Buch, Verweise auf andere Anhänge auf die übrigen Dokumente des Werkzeugkastens. Alle zehn Anhänge: www.amazing-agents.com/predictable.

It's predictable when you do the math.

AMAZING AGENTS

Pirmasens · 2026

www.amazing-agents.com