

Wer kontrolliert den Code?

Datenschutzrechtliche Systempflichten bei KI-gestützter Softwareentwicklung

Dr. Moritz Indenhuck · Lennart Perkowski

lindenpartners

Herbstakademie 2026

Gliederung

I

Warum Art. 25 DSGVO durch Coding Agents an Bedeutung gewinnt

Agentische Entwicklung · Beispielsfall Bewerberportal

II

Art. 25 als Systemgestaltungs- und Gewährleistungspflicht

Pflichtzeitpunkte · Voreinstellungen · Risikobasierung

III

Die Kontrollkette der agentischen Entwicklung

Auswahl · Gestaltung · Entwicklung · Freigabe · Betrieb

IV

CRA und Stand der Technik

Security by Design als Auslegungshilfe

V

Fazit: Wer kontrolliert den Code?



Warum Art. 25 DSGVO durch Coding Agents an Bedeutung gewinnt



I · Ausgangslage

II · Art. 25 als Systempflicht

III · Die Kontrollkette

IV · CRA und Stand der Technik

V · Fazit

Vom Vibe Coding zur agentischen Entwicklung

I

„Man solle sich den Vibes hingeben – und vergessen, dass der Code überhaupt existiert.“

Andrej Karpathy, Februar 2025

Was ein Coding Agent selbständig tut

Repository lesen

Arbeitsschritte planen

Dateien verändern

Bibliotheken installieren

Tests ausführen

Fehler verarbeiten

↻ und setzt seine Arbeit selbständig fort

Zunehmend erhält der Agent nur noch eine Beschreibung des Problems und liefert eine funktionsfähige Anwendung zurück. Organisationen entwickeln damit in kurzer Zeit eigene Anwendungen, die früher ein klassisches Entwicklungsprojekt erfordert hätten.

Beispielsfall: das Bewerberportal

AUFTRAG DER PERSONALABTEILUNG AN DEN CODING AGENT

„Erstelle ein Portal mit Bewerbungsformular, Kalenderanbindung und einer Übersicht für die Fachbereiche.“

Der Auftrag beschreibt eine Funktion. Offen bleibt:



Welche Bewerberdaten sind für welchen Zweck erforderlich?



Wer darf sie erhalten?



Wie lange werden sie gespeichert?



Bewertet das Portal Bewerbungen oder übermittelt es sie nur?

Die Organisation entscheidet nicht nur, welches System sie verwendet. Sie veranlasst, wie die spätere Verarbeitung technisch eingerichtet wird.

Wo Art. 25 ansetzt

I

Standardsoftware

Architektur ist weitgehend vorgegeben

Auswahl des Anbieters

Konfiguration

Kontrolle im Betrieb

Agentische Eigenentwicklung

Der Verantwortliche tritt in den Gestaltungsprozess ein

Auswahl des Entwicklungswerkzeugs

Gestaltung der Verarbeitung

Entwicklung und Freigabe

Erhaltung im Betrieb

Art. 25 wird damit von einer Auswahl- und Konfigurationspflicht zu einer unmittelbaren Vorgabe für Gestaltung, Entwicklung und Freigabe.

Beleg: Art. 25 Abs. 1 DSGVO; EDSA, Leitlinien 4/2019 zu Art. 25 DSGVO, Rn. 33–39.



Art. 25 als Systemgestaltungs- und Gewährleistungspflicht

I · Ausgangslage

II · Art. 25 als Systempflicht

III · Die Kontrollkette

IV · CRA und Stand der Technik

V · Fazit

Zwei Pflichtzeitpunkte des Art. 25 Abs. 1

II

Der Wortlaut erfasst neben der Verarbeitung selbst ausdrücklich auch die Festlegung ihrer Mittel. Die Pflichtenbindung wird damit in die Softwareentwicklung vorverlagert, soweit das Vorhaben hinreichend konkret auf eine spätere Verarbeitung ausgerichtet ist.

Festlegung der Mittel

Auswahl · Gestaltung · Entwicklung · Freigabe — vor der ersten Verarbeitung personenbezogener Daten

Verarbeitung

Betrieb — fortlaufende Erhaltung und Überprüfung der Maßnahmen

Art. 25 erweitert nicht den sachlichen Anwendungsbereich der DSGVO. Er knüpft an eine beabsichtigte Verarbeitung an und bestimmt die Festlegung der Mittel ausdrücklich als vorgelagerten Pflichtzeitpunkt.

Spätestens mit Beginn der vorgesehenen Verarbeitung muss das System den Anforderungen entsprechen — und der Verantwortliche nachweisen können, dass er die Maßnahmen bereits bei der Festlegung der Mittel getroffen hat.

Vom Grundsatz zur Systemeigenschaft

II

Nicht nur am einzelnen Verarbeitungsvorgang prüfen, sondern in Logik und Architektur des Systems einbauen.

DATENSCHUTZGRUNDSATZ

Datenminimierung

→

begrenztes Datenmodell

Speicherbegrenzung

→

Löschlogik

Zweckbindung

→

begrenzte Funktionen und Datenflüsse

Betroffenenrechte

→

auffindbare, berichtigungs-, export- und löschfähige Datensätze

Vertraulichkeit

→

Rollen, Berechtigungen, technische Abschottung

Beleg: EDSA, Leitlinien 4/2019, Rn. 33–39; BeckOK DatenschutzR/Paulus/Schmidt, Art. 25 Rn. 4–7; Gola/Heckmann/Baumgartner, Art. 25 Rn. 13–20.

Art. 25 Abs. 2: vier Dimensionen der Voreinstellung

II

Standardmäßig dürfen nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten verarbeitet werden.

Datenmenge

Welche Formularfelder werden eingeblendet oder verpflichtend abgefragt?

Verarbeitungsumfang

Verwaltet das Portal Bewerbungen — oder bewertet es sie auch?

Speicherdauer

Welche Aufbewahrungsdauer ist systemseitig voreingestellt?

Zugänglichkeit

Für welche Fachbereiche ist eine Bewerbung sichtbar?

Voreinstellung ist eine Entwurfsentscheidung — sie fällt im Code, nicht im Betrieb.

Art. 25 Abs. 2 verdichtet die Gestaltungspflicht: Für jede der vier Dimensionen muss die Voreinstellung begründet auf das Erforderliche begrenzt sein.

Eigenständiger Gehalt — und Risikobasierung

II

Rechtliche Vorgabe

Art. 25 schließt die Lücke

Technische Vollziehbarkeit

Beispiel Löschung: Solange keine Frist abgelaufen und kein Löschungsbegehren gestellt ist, müssen Art. 5 Abs. 1 lit. e und Art. 17 noch nicht verletzt sein. Fehlt aber architekturbedingt jede verlässliche Möglichkeit, Hauptdaten, Protokolle und weitere Kopien fristgerecht zu löschen, fehlt schon die von Art. 25 verlangte Gewährleistung.

Risikobasierter Maßstab

Stand der Technik

Implementierungskosten

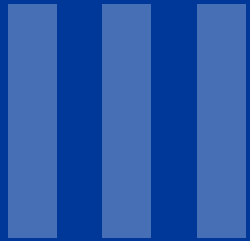
Art, Umfang, Umstände und
ZweckeWahrscheinlichkeit und
Schwere der Risiken

EuGH zu Art. 24 und 32: Weder beweist ein Vorfall automatisch die Ungeeignetheit der Maßnahmen, noch genügt ihre abstrakte Behauptung. Maßgeblich ist die konkrete Prüfung — derselbe Wirksamkeitsgedanke prägt Art. 25.

Beleg: EuGH, Urt. v. 14.12.2023 – C-340/21, Natsionalna agentsia za prihodite, Rn. 29–32, 45–47, 52–57; Art. 58 Abs. 2 lit. a DSGVO.

Art. 25 verpflichtet den Verantwortlichen, den materiellen Sollzustand der DSGVO rechtzeitig in wirksame Eigenschaften des Verarbeitungssystems zu übersetzen.

Diese Pflicht steht in einem Spannungsverhältnis zur KI-gestützten Softwareentwicklung.



Die Kontrollkette der agentischen Entwicklung

I · Ausgangslage

II · Art. 25 als Systempflicht

III · Die Kontrollkette

IV · CRA und Stand der Technik

V · Fazit

Die Kontrollkette im Überblick

III

Coding Agents erzeugen Lösungen probabilistisch — gesteuert von Trainingsdaten, Nachtraining, System- und Projektanweisungen, Repository-Kontext, Werkzeugen und Tests. Die Vorgaben des Art. 25 sind dabei kein gesonderter Maßstab.

1**Auswahl**

Beherrschbares
Entwicklungsmodell
wählen

Grenzen bestimmen

2**Gestaltung**

Normativen
Sollzustand festlegen

Sollzustand festlegen

3**Entwicklung**

Vorgaben wirksam
umsetzen

in Technik übersetzen

4**Freigabe**

Umsetzung materiell
kontrollieren

Einhaltung prüfen

5**Betrieb**

Wirksamkeit erhalten

Wirksamkeit erhalten

Verantwortlich bleibt die Organisation, die den Agenten einsetzt und seine Entscheidungsspielräume bestimmt — oder ungeregelt lässt.

1. Auswahl: ein beherrschbares Entwicklungsmodell wählen

1 Auswahl

2 Gestaltung

3 Entwicklung

4 Freigabe

5 Betrieb

Die Auswahlentscheidung fällt nicht weg. Zunächst: beschaffen oder selbst entwickeln? Bei agentischer Entwicklung tritt die Wahl des Werkzeugs hinzu. Der EDSA ordnet Beschaffung und Implementierung ausdrücklich der Mittelfestlegung zu.

Datenschutzrelevante Eigenschaften des Werkzeugs

Steuerbarkeit

Berechtigungs-
konzept

Protokollierung

Abschottung der
Ausführungs-
umgebungVerbindliche
Projektvorgaben

Die Entscheidung darf sich nicht allein an Geschwindigkeit, Kosten oder allgemeiner Codequalität orientieren. Bei erheblichen Unterschieden und im Übrigen vergleichbaren Einsatzbedingungen kann die Wahl des datenschutzrechtlich zuverlässigeren Modells geboten sein.

2. Gestaltung: den normativen Sollzustand festlegen

1 Auswahl

2 Gestaltung

3 Entwicklung

4 Freigabe

5 Betrieb

Wesentliche Mittel — Entscheidung des Verantwortlichen

Kategorien betroffener Personen
und Daten

Empfänger

Speicherdauer

Der Agent darf

ein geeignetes Eingabeelement für ein bereits festgelegtes Datenfeld wählen und technische Einzelheiten ausführend konkretisieren.

Der Agent darf nicht

faktisch entscheiden, welche personenbezogenen Daten für den Einstellungszweck erforderlich sind.

Erst die **Verarbeitungsspezifikation** gibt dem Agenten und der späteren Kontrolle einen rechtlichen Maßstab. Ein offener Entwicklungsauftrag delegiert nicht nur Programmierarbeit — er unterlässt die Festlegung.

3. Entwicklung: rechtliche Vorgaben wirksam umsetzen

1 Auswahl

2 Gestaltung

3 Entwicklung

4 Freigabe

5 Betrieb

Der Sollzustand muss den Agenten steuern, in datenschutzfähige Funktionen übersetzt und in einer abgesicherten Umgebung umgesetzt werden.

AUFGABE 1

Prompt-Governance

Wer darf den Agenten einsetzen?
Welche Verarbeitungsspezifikation ist zwingend Teil des Kontexts?
Welche Entscheidungen bedürfen gesonderter Freigabe?

Fachkonzepte, Projektanweisungen, maschinenlesbare Policies, Abnahmekriterien.

AUFGABE 2

Umsetzung im Portal

Freigegebenes Datenmodell, rollenbasierte Zugriffe, sparsame Voreinstellungen, belastbare Prozesse für Löschung und Betroffenenrechte.

Keine zusätzlichen Datenkategorien, keine ungenehmigten Empfänger, keine automatische Rangbildung.

AUFGABE 3

Sicherheit der Entwicklung

Beschränkte Repository-, Ausführungs- und Deploymentrechte, Trennung von Entwicklung und Produktion, freigegebene Paketquellen.

Geheimnis- und Abhängigkeitsprüfungen.

Art. 25 wirkt damit auch auf die Organisation des Entwicklungsprozesses.

Beispiel: Slopsquatting

1

Der Coding Agent schlägt ein Softwarepaket vor, das nicht existiert.

2

Ein Angreifer registriert diesen erfundenen Paketnamen und veröffentlicht darunter Schadsoftware.

3

Der Agent installiert automatisiert gerade dieses manipulierte Paket.

4

Die eingeschleuste Software erhält Zugriff auf Bewerberdaten — Vertraulichkeit und Integrität sind gefährdet.

Die Absicherung ist kein allgemeines Misstrauensvotum gegen Coding Agents, sondern eine an einem konkreten Risiko ausgerichtete Systemmaßnahme nach Art. 25 und 32 DSGVO.

Freigegebene Paketquellen

Abhängigkeitsprüfungen

Getrennte Umgebungen

4. Freigabe: die Umsetzung materiell kontrollieren

1 Auswahl

2 Gestaltung

3 Entwicklung

4 Freigabe

5 Betrieb

Abgleich mit dem Sollzustand

Entspricht das Datenbankschema den freigegebenen Datenkategorien?

Stimmen Datenflüsse und Berechtigungen mit den festgelegten Empfängern überein?

Funktioniert die Löschung für sämtliche relevanten Speicherorte?

Human in the Loop — nur wirksam bei

Prüfkriterien

Informationsgrundlage

Qualifikation

Zeit

Entscheidungskompetenz

Keine Zeile-für-Zeile-Lektüre gefordert: aussagekräftige Schema-, Datenfluss-, Rollen- und Löschtests können die Kontrolle tragen.

CODE WITH CLAUDE, MAI 2026

Fast die Hälfte der Anwesenden hatte in der Vorwoche einen vollständig von Claude geschriebenen Pull Request ausgeliefert. Auf die Nachfrage, wer den Code nicht gelesen habe, blieb die Mehrzahl dieser Hände oben.

Die Freigabeentscheidung ist nachvollziehbar zu dokumentieren: Vorgaben, Prüfungen, verbliebene Abweichungen, Freigabegründe.

Beleg: Heaven, MIT Technology Review v. 21.5.2026; Art. 5 Abs. 2, Art. 24 Abs. 1, Art. 25 Abs. 1 DSGVO; EDSA, Leitlinien 4/2019, Rn. 15–16 und 86–88.

5. Betrieb: die Wirksamkeit erhalten

1 Auswahl

2 Gestaltung

3 Entwicklung

4 Freigabe

5 Betrieb

Die Freigabe ist nicht der Abschluss der Systemverantwortung, sondern der Übergang von der vorgelagerten Gestaltungspflicht in eine fortlaufende Erhaltungs- und Überprüfungspflicht.

Auslöser einer erneuten Prüfung

Neue Schnittstelle zu einem
Kalenderdienst

Erweiterte Berechtigungen

Agenten-Update ergänzt eine
automatische Auswertung von
Bewerbungsunterlagen

↻ Zweck · Datenflüsse · Risiken · Stand der Technik neu bewerten

Solche Änderungen lösen eine erneute Prüfung der Verarbeitungsspezifikation und der Wirksamkeit der Maßnahmen aus.

IV

CRA und Stand der Technik

I · Ausgangslage

II · Art. 25 als Systempflicht

III · Die Kontrollkette

IV · CRA und Stand der Technik

V · Fazit

CRA und Stand der Technik

Cyber Resilience Act

Produktsicherheitsrechtliche Pflichten für Produkte mit digitalen Elementen. Eigener Anwendungsbereich, Grundsatz der Security by Design.



Art. 25 DSGVO

Technische und organisatorische Maßnahmen nach dem Stand der Technik, bezogen auf die Verarbeitung personenbezogener Daten.

Die Kommission stellt klar: Eine Einhaltung des CRA impliziert keine Einhaltung der DSGVO — und umgekehrt.

Brücke: der Stand der Technik

Soweit der CRA den Stand der Technik im Bereich der IT-Sicherheit normiert, liegt es nahe, ihn bei der Bestimmung der Maßnahmen nach Art. 25 Abs. 1 heranzuziehen. Künftige Standards zur agentischen Entwicklung könnten dort Anforderungen genauer konturieren:

Sandboxen

Berechtigungen

Paketquellen

Freigabebeschränken



Fazit: Wer kontrolliert den Code?

I · Ausgangslage

II · Art. 25 als Systempflicht

III · Die Kontrollkette

IV · CRA und Stand der Technik

V · Fazit

Fünf Schritte für den Verantwortlichen

Art. 25 führt keine neuen materiellen Anforderungen ein. Sein Eigengehalt ist prozedural: Die Anforderungen der DSGVO werden in die Festlegung und technische Umsetzung der Verarbeitungsmittel verlagert.

- 1 Ein hinreichend steuerbares Entwicklungswerkzeug auswählen
- 2 Den rechtlich zulässigen Möglichkeitsraum durch eine Verarbeitungsspezifikation festlegen
- 3 Den Coding Agent verbindlich instruieren
- 4 Den erzeugten Output vor der Freigabe materiell kontrollieren
- 5 Die Wirksamkeit der Maßnahmen im Betrieb erhalten

Die Kontrolle beginnt, bevor die erste Zeile Code geschrieben wird. Der funktionale Entwicklungsauftrag allein genügt nicht.

Kontrolle im Sinne des Art. 25 DSGVO besteht in der Beherrschung der durch den Code hervorgebrachten Verarbeitung.

Je selbständiger ein Coding Agent die technische Implementierung übernimmt, desto weniger kann diese Beherrschung auf der persönlichen Kenntnis des Codes beruhen — und desto stärker muss sie durch verbindliche Systemvorgaben, technische Grenzen und materielle Kontrollen institutionell abgesichert werden.

Dr. Moritz Indenhuck · Lennart Perkowski — lindenpartners