

# Leitfaden für die Selbstbewertung von Systemen künstlicher Intelligenz (KI)

Die CNIL schlägt ein Analyseraster vor, damit Organisationen die Reife ihrer KI-Systeme im Hinblick auf die DSGVO selbst bewerten können. Außerdem stellt sie bewährte Verfahren vor.

## Einleitung: Was Sie wissen sollten, bevor Sie den Leitfaden lesen

Der auf den folgenden Seiten vorgeschlagene Leitfaden zur Selbstbewertung soll die wichtigsten Fragen zum Datenschutz in den meisten auftretenden Fällen in Erinnerung rufen.

Die CNIL fordert alle Organisationen (Anbieter oder Nutzer von KI-Systemen), die eine Verarbeitung mithilfe von Technologien der künstlichen Intelligenz (KI) planen oder dies bereits eingeleitet haben, dazu auf, sich die in diesem Analyseraster vorgeschlagenen Fragen zu stellen.

Die Liste wurde so umfassend wie möglich auf der Grundlage von bewährten Verfahren und aufkommenden Signalen aus der wissenschaftlichen Forschung in diesem Bereich zusammengestellt. Damit sie auf alle Branchen und Arten von KI-Systemen anwendbar ist, wurden die Bögen so gestaltet, dass sie möglichst viele Fälle abdecken, ohne die Risiken bestimmter Techniken wie kontinuierliches Lernen oder maschinelle Annotation auszuschließen.

Das Ziel dieses Rasters ist es, eine Selbstbewertung aller relevanten datenschutzrechtlichen und ethischen Aspekte eines Verarbeitungsprojekts zu ermöglichen. Eine Funktionsanalyse durch die CNIL kann nur im Rahmen einer formellen Anfrage, z. B. im Rahmen eines Beratungsantrags, durchgeführt werden. Dieses Raster erfüllt einen informativen Zweck, hauptsächlich unter dem Gesichtspunkt des Schutzes personenbezogener Daten. Es ist nicht dazu gedacht, andere anwendbare Texte zu verdrängen: sektorale Gesetze, zivilrechtliche Haftungsregelungen usw.

In diesen Arbeitsblättern werden die Begriffe "Anbieter" und "Nutzer" von KI-Systemen verwendet. Die CNIL legt folgende Definitionen zugrunde:

### Anbieter

Der Anbieter ist eine natürliche oder juristische Person, Behörde, Agentur oder sonstige Einrichtung, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke entgeltlich oder unentgeltlich auf den Markt zu bringen oder in Betrieb zu nehmen.

### Nutzer

Jede natürliche oder juristische Person, Behörde, Agentur oder andere Organisation, die unter ihrer eigenen Autorität ein KI-System nutzt, außer wenn das System im Rahmen einer persönlichen, nicht beruflichen Tätigkeit genutzt wird.

### Endnutzer

Der Nutzer des KI-Systems darf nicht mit dem Endnutzer verwechselt werden, d. h. der Person, die von dem System betroffen ist: Der Begriff der Nutzung entspricht somit einer Nutzung in einem beruflichen Rahmen.

Gemäß den Definitionen der DSGVO können Anbieter und Nutzer als für die Verarbeitung Verantwortliche und/oder Auftragsverarbeiter fungieren, wenn das KI-System personenbezogene Daten verarbeitet.

Diese Analyse der Rollen und Verantwortlichkeiten muss von Fall zu Fall durchgeführt werden, wie in den Arbeitsblättern beschrieben.

Arbeitsblatt 1: Stellen Sie sich die richtigen Fragen, bevor Sie ein System mit künstlicher Intelligenz einsetzen

Integrieren Sie KI auf verhältnismäßige Weise und mit einem klaren Ziel.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/01\\_Die-richtigen-Fragen-stellen.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/01_Die-richtigen-Fragen-stellen.pdf)

Arbeitsblatt 2: Sammeln und qualifizieren Sie Trainingsdaten

Beachten Sie bei der Erhebung die DSGVO und bauen Sie eine qualitativ hochwertige Datenbank auf.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/02\\_Sammeln-und-Qualifizieren-von-Trainingsdaten.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/02_Sammeln-und-Qualifizieren-von-Trainingsdaten.pdf)

Arbeitsblatt 3: Einen Algorithmus entwickeln und trainieren

Setzen Sie in dieser entscheidenden Phase bewährte Verfahren ein.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/03\\_Algorithmus-entwickeln-und-trainieren.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/03_Algorithmus-entwickeln-und-trainieren.pdf)

Arbeitsblatt 4: Ein KI-System in der Produktion einsetzen

Gewährleistung der Qualität und Transparenz des Systems während des Einsatzes.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/04\\_KI-System-in-der-Produktion-einsetzen.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/04_KI-System-in-der-Produktion-einsetzen.pdf)

Arbeitsblatt 5: Sichern Sie die Verarbeitung ab

Analysieren Sie Risiken und verhindern Sie Schwachstellen und Angriffe.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/05\\_Die-Verarbeitung-absichern.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/05_Die-Verarbeitung-absichern.pdf)

Arbeitsblatt 6: Ermöglichen Sie den Personen die ordnungsgemäße Ausübung ihrer Rechte

Fördern Sie die Transparenz und die Rechte der Endnutzer.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/06\\_Betroffenenrechte-umsetzen.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/06_Betroffenenrechte-umsetzen.pdf)

## Arbeitsblatt 7: Die Einhaltung der Vorschriften sicherstellen

Weisen Sie Verantwortlichkeiten zu und dokumentieren Sie Ihre Verarbeitung.

- **Zum Arbeitsblatt:** [https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/07\\_Einhaltung-der-Vorschriften-sicherstellen.pdf](https://www.datenschutz-praxis.de/wp-content/uploads/sites/2/2022/04/07_Einhaltung-der-Vorschriften-sicherstellen.pdf)

Weitere Leitfäden, Tools und Best Practices: <https://www.cnil.fr/fr/intelligence-artificielle/guide/conformite-des-systemes-dia-les-autres-guides-outils-et-bonnes-pratiques>