Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# KI, Datenschutz und öffentliche Verwaltung - Vertiefung

“Digi-Lunch” 18.7.2024

Prof. Dr. Tobias Keber

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg

# …was bisher geschah

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

**Ein Elephant sitzt in einem Serverraum und versteckt sich hinter Kabeln**

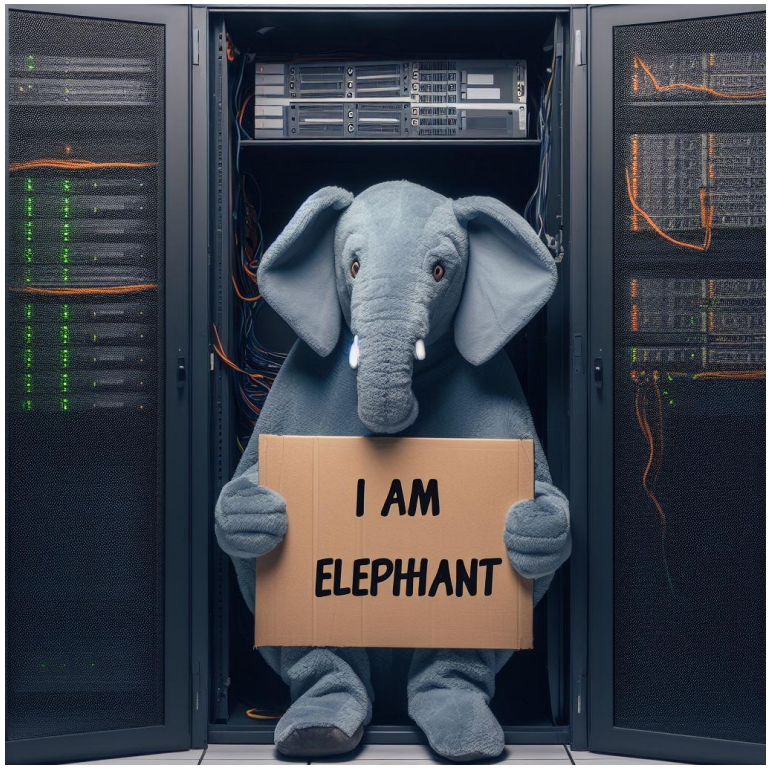
Bing Image Creator | 1024 × 1024 jpg | Jetzt erstellt

Teilen Speichern Herunterladen Feedback

Inhaltsnachweise
**Mit KI erstellt** · 13. November 2023 um 6:55 PM

# Betroffenenrechte und Transparenz. Wie?

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg



# Überblick über die KI-VO

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

## Produkthaftungsgesetz

→ guten Überblick bietet:
https://artificialintelligenceact.eu/de/

- 13 Kapitel mit 113 Artikel
- 180 Erwägungsgründe
- 8 Anhänge
- die aktuelle PDF-Version hat einen Umfang von 460 Seiten
- „Produkthaftungsvorschriften“

# 1.: die KI-VO ist da.
# …aber darum geht es heute nicht.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# “ONKIDA”

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

## Orientierungshilfen-Navigat@r KI & Datenschutz (ONKIDA)

Fundstellenübersicht zu zehn zentralen Vorgaben des Datenschutzrechts in aufsichtsbehördlichen Orientierungshilfen zu „Künstlicher Intelligenz“. Stand Juli 2024.

| | A. EDPS Guidelines on generative AI and the EUDPR (2024, PDF) Datenverarbeitung durch EU-Organe | B. Report der EDSA Taskforce ChatGPT (2024, PDF) | C. DSK: Orientierungshilfe zu KI und Datenschutz (2024, PDF) | D. LfDI BW: Rechtsgrundlagen zum Einsatz von KI (2023) | E. BayLDA: Checkliste Datenschutz-konforme KI (2024, PDF) | F. Hamburger BfDI: Checkliste zum Einsatz LLM-basierter Chatbots (2023, PDF) | G. CNIL: Recommendations on the development of AI systems („How-to sheets“) (2024) | H. DSB Österreich: FAQ KI und Datenschutz (2024) | I. DSK: Positionspapier zu TOM bei Entwicklung und Betrieb von KI-Systemen (2019, PDF) | J. DSK: Hambacher Erklärung zur KI (2019, PDF) |
|---|---|---|---|---|---|---|---|---|---|---|
| **1. Grundsatz der Datenrichtigkeit** Art. 5 I lit. d) DSGVO | (+) S. 15 f. (Art. 4 I lit. d) VO 2018/1725) | (+) Rn. 29 ff. sowie im Fragebogen im Annex, S. 11 | (+/−) Recht auf Berichtigung Rn. 27, Überprüfung der Richtigkeit der Ergebnisse Rn. 64 f. | (−) | (+/−) Recht auf Berichtigung, S. 6, 10 | (+/−) Überprüfung der Richtigkeit des Ergebnisses S. 4 | (+/−) „data cleaning“, „relevant data“, „monitoring and updating“ Sheet 7 | (+) | (+/−) Heranziehung falscher Rohdaten S. 10, Training mit geeigneten Daten S. 11 | (−) |
| **2. Grundsatz der Datenminimierung** Art. 5 I lit. c) DSGVO **Zweckbindungs-grundsatz** Art. 5 I lit. b) DSGVO | (+) Datenminimierung: S. 14 (Art. 4 I lit. c) VO 2018/1725) (+/−) Zweckbindung: nur sehr indirekt („consistent with original purpose“), S. 12 | (+/−) nur im Rahmen des Fragebogens im Annex, S. 10 | (+) Zweckbindung Rn. 1 f. | (+/−) Berücksichtigung Datenminimierung bei Art. 6 I lit. f DSGVO (S. 17) u. § 13 LDSG BW (S. 25) (+) Zweckänderung S. 15 | (+/−) Zweckbindung nur eher indirekt S. 6, 8, 11 (Checkliste) | (−) | (+) Sheet 2, Datenminimierung auch Sheet 6, Zweckkompatibilität auch Sheet 4 (2/2) | (+) | (+) Datenminimierung S. 9, 14, 17 (+) Zweckbindung S. 6 f., 7 (Fragebogen), 8, 9, 14, 17 | (+) Datenminimierung, S. 4 (+) Zweckbindung S. 3; |
| **3. Personenbezug** Art. 4 Nr. 1 DSGVO | (+) S. 7 (Art. 3 Nr. 1 VO 2018/1725) | (−) | (+) Rn. 4 ff., 7 f., 48 ff. | (+) insbes. S. 6 | (+) S. 4, 5, 9,10, 11 (Checklisten) | (+) S. 2 f. *vgl. auch Hamburger Thesen zum Personenbezug in Large Language Models v. 15.7.2024* | (+) Introduction | (−) | (+) S. 15 kurzer Satz im Zusammenhang mit Vertraulichkeit beim Training | (−) |
| **4. Rechtsgrundlagen für die Datenverarbeitung** Art. 6 I u. 9 II DSGVO | (+) S. 11 ff. (Art. 5 und 10 II VO 2018/1725) | (+) Rn. 13 ff., ebenso im Fragebogen S. 12 f. | (+) Rn. 9 ff. (zudem Verweis auf Positionspapier LfDI BW), Rn. 62 (im Zusammenhang mit sensiblen Daten) | (+) insbes. S. 11 ff. | (+) S. 4 und 9 (Checklisten) | (+) S. 2 (indirekt im Zusammenhang mit Personenbezug) und S. 4 (im Zusammenhang mit Diskriminierung) | (+) Sheet 4 (1/2 und 2/2) | (+/−) nur allgemeine Bezugnahme | (+/−) vereinzelt kurze Bezugnahmen, dass es einer Rechtsgrundlage bedarf | (−) |
| **5. (Mit−)Verantwortlichkeit** Art. 26 (und 28) DSGVO | (+) S. 6 | (+/−) Rn. 23 ff. in Zusammenhang mit Fairness-Prinzip, „Abwälzung“ der Verantwortlichkeit auf betroffene Personen; im Rahmen des Fragebogens S. 14 | (+) Rn. 32 ff. | (+) S. 9 ff. | (+) S. 9 | (−) | (+) Sheet 3 | (−) | (+/−) indirekt: Klärung der Zugriffsmöglichkeiten von Cloud-Anbietern S. 16; „Rollen- und Berechtigungskonzept“ S. 15,18,19 | (+/−) S. 4 (nur knappe Bezugnahme auf Ermittlung der Verantwortlichkeit) |
| **6. Transparenzgebot und Informationspflichten** Art. 5 I lit. a und 12 ff. DSGVO | (+) S. 17 (Art. 14 VO 2018/1725) | (+) Rn. 27 f., ebenso im Fragebogen S. 13 | (+) Rn. 21 ff. | (+) S. 12 (im Zusammenhang mit informierter Einwilligung) | (+) Transparenz S. 7 (als Teil des „Datenschutz-Risikomodells“) (+) Infopflichten S. 5 (Checkliste) | (−) | (+) Sheet 2, Dokumentation in Sheet 7 | (+) | (+) S. 5, 11 ff., 16 f. | (+) S. 3 |
| **7. Auskunftsanspruch** Art. 15 DSGVO **Recht auf Löschung** Art. 17 DSGVO | (+/−) allgemein Betroffenenrechte S. 22 | (+) allgemein Betroffenenrechte Rn. 32 ff. | (+) nur Recht auf Löschung Rn. 26, 28 f.; „weitere Betroffenenechte“ Rn. 30 | (+) nur Recht auf Löschung S. 12 | (+) Auskunftsanspruch S. 5, 10 (Checkliste), Recht auf Löschung S. 6, 10 (Checkliste) | (−) | (−) | (+/−) nur allgemeine Bezugnahme auf Betroffenenrechte | (+) Auskunftsanspruch, S. 7; Betroffenenrechte allgemein S. 18 (in einem Satz) | (−) |
| **8. Automatisierte Entscheidungen und Profiling** Art. 22 DSGVO | (+) S. 18 (Art. 24 VO 2018/1725) | (−) | (+) Rn. 12 ff. | (−) | (−) | (+) S. 22 | (−) | (+) | (+) S. 5 (mehr oder weniger), S. 14 (Bezugnahme in einem Satz, indirekt), S. 18 | (+) S. 3 |
| **9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen** Art. 25 DSGVO | (+) S. 9 (Art. 27 VO 2018/1725) | (+) Rn. 7 knappe Bezugnahme; Rn. 35 im Zusammenhang mit Betroffenenrechten | (+) Rn. 43 | (+/−) S. 7 (Bewertung Personenbezug), S. 18 Fn. 57 (Berücksichtigung bei Art. 6 I lit. f DSGVO) | (+), S. 7 (nur ein knapper Satz) | (−) | (+) Sheet 6 (Vorschrift wird nicht direkt genannt, aber Konzept DPbD wird beschrieben), Sheet 7 | (−) | (+) S. 7 (analog?) | (+) S. 2, 4 |
| **10. Datenschutz-Folgenabschätzung** Art. 35 DSGVO | (+) S. 9 f. (Art. 39 u. 89 VO 2018/1725) | (+/−) nur im Rahmen des Fragebogens im Annex, S. 11 | (+) Rn. 38 ff. | (−) | (+) S. 4, 6, 9, 11 (Checklisten), S. 7 | (+) S. 2 | (+) Sheet 5 | (−) | (+) S. 5 | (+) S. 4 |

https://www.baden-wuerttemberg.datenschutz.de/onki

# …seit heute online

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

https://www.baden-wuerttemberg.datenschutz.de/onkida/

# Agenda

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

1. Datenrichtigkeit
2. Datenminimierung und Zweckbindung
3. Personenbezug
4. Rechtsgrundlagen
5. (Mit)Verantwortlichkeit
6. Transparenz und Informationspflichten
7. Auskunftsanspruch und Recht auf Löschung
8. Automatisierte Entscheidung und Profiling
9. Datenschutz durch Technikgestaltung
10. Datenschutz-Folgenabschätzung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

## Akteure

- EDPS [A.]
- EDSA [B.]
- DSK [C.,I.,J.]
- LfD[I]s .de [D.,E.,F.]
- Aufsichtsbehörden .fr, .at [G.,H.]

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 1. DATENRICHTIGKEIT

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 1. Datenrichtigkeit

Art. 5
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

[...]

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden ("Richtigkeit").

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 1. Datenrichtigkeit

B.„Report of the work undertaken by the ChatGPT Taskforce“ des EDSA vom 23. Mai 2024

3.4 Data Accuracy (Rn. 29 ff.)

In relation to the principle of data accuracy pursuant to Article 5(1)(d) GDPR, a difference should be made between input and output data. Input data can encompass either data collected, for instance, through web scraping or the “Content” provided by data subjects when using ChatGPT (such as “prompts”). Output data encompasses the output following the interactions with ChatGPT.

It has to be noted that the purpose of the data processing is to train ChatGPT and not necessarily to provide factually accurate information. [...] In any case, the principle of data accuracy must be complied with.

[...] Although the measures taken in order to comply with the transparency principle are beneficial to avoid misinterpretation of the output of ChatGPT, they are not sufficient to comply with the data accuracy principle.

+ 4. ANNEX (QUESTIONNAIRE) - Fragenkatalog unter II. d) „Principles relating to processing of personal data“ (Seite 11)

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 1. Datenrichtigkeit

C. Orientierungshilfe der DSK zu „Künstlicher Intelligenz und Datenschutz“ vom 6. Mai 2024:

Nummer 1.11, Rn. 27: Berichtigung, Löschung und weitere Betroffenenrechte
„Beim Einsatz von KI-Anwendungen kann es aus unterschiedlichen Gründen dazu kommen, dass unrichtige personenbezogene Daten verarbeitet werden. [...] . Hinsichtlich personenbezogener Daten besteht bei *Unrichtigkeit* jedoch ein Recht der betroffenen Personen auf Berichtigung. Diese Berichtigung muss in einer KI-Anwendung umsetzbar sein, zum Beispiel durch Korrektur von Daten oder durch ein Nachtraining/Fine Tuning.“

Nummer 3.3, Rn. 64, 65: Ergebnisse auf Richtigkeit prüfen
„Die Ergebnisse von KI-Anwendungen mit Personenbezug müssen kritisch hinterfragt werden. [...] erzeugten Texte keinen Anspruch auf Richtigkeit haben und stets hinterfragt werden sollten. Überdies können KI-Anwendungen unterschiedliche Informationsstände haben.
Im Hinblick auf personenbezogene Ergebnisse oder eine personenbezogene Anwendung der Ergebnisse können unrichtige Ergebnisse aber zu unzulässigen Verarbeitungen führen, [...].“

# 1. Datenrichtigkeit

G. Sheet 7 „Taking data protection into account in data collection and management“ der „AI how-to sheets“ der CNIL :

Reiter „Data cleaning, data identification and privacy by design“

- **Data cleaning**

  „Data cleaning helps in creating a quality training dataset. This is a crucial step that strengthens data integrity and relevance by reducing inconsistencies, as well as the cost of training. Specifically, it consists in:

  [...] correcting errors; [...]“

- **Monitoring and updating**

  Although [...] data protection measures have been implemented during data collection, these measures may become obsolete over time. The data collected could lose their exact, [...] adequate and limited character, in particular because of: [...]

  - changes in the relationship between characteristics;
  - malicious poisoning as part of continuous learning, which can for example be noticed by abnormal outcomes.

  Tools exist to detect the occurrence of data drift, [...] can be used for this purpose;

  - an update of the data, such as a correction of the place of residence in the public profile of the user of a social network following a move; [...]

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 1. Datenrichtigkeit

H. „FAQ zum Thema KI und Datenschutz“ Österreichischen Datenschutzbehörde

7. Welche datenschutzrechtlichen Verpflichtungen sind beim Einsatz von KI-Systemen zu beachten?

[...] Richtigkeit:

Der Grundsatz der Datenrichtigkeit besagt, dass Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen und dabei alle angemessenen Maßnahmen zu treffen sind, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Dies ist gerade bei (text-)generierenden Systemen regelmäßig mit Herausforderungen verbunden, da bei aktuell vorhandenen Systemen üblicherweise ein Output generiert wird, der aus statistischer Sicht am wahrscheinlichsten, jedoch nicht notwendigerweise sachlich richtig ist.

In Anbetracht dessen sind betroffene Personen jedenfalls darüber zu informieren, dass die von derartigen Systemen erzeugten Ergebnisse irreführend und falsch sein können.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 2. DATENMINIMIERUNG UND ZWECKBINDUNG

# 2. Datenminimierung und Zweckbindung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

**Art. 5**
**Grundsätze für die Verarbeitung personenbezogener Daten**

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken ("Zweckbindung");

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("Datenminimierung");

# 2. Datenminimierung und Zweckbindung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

C. DSK Orientierungshilfe, Rn. 1 f.

„Vor dem Einsatz einer KI-Anwendung sollten Verantwortliche explizit festlegen, welche Einsatzfelder für die KI-Anwendung vorgesehen sind und welchem Zweck diese konkret dient. Im Hinblick auf die Verarbeitung personenbezogener Daten ist diese Zweckfestlegung elementar für den datenschutzkonformen Betrieb, da nur aufgrund konkreter vorab festgelegter Zwecke überprüft werden kann, ob die Verarbeitung personenbezogener Daten zur Zweckerreichung erforderlich ist.“

„Für öffentliche Stellen ist es diesbezüglich auch wichtig, sicherzustellen, dass sich das Einsatzfeld im Rahmen der ihnen gesetzlich zugewiesenen öffentlichen Aufgaben befindet [...].“

# 2. Datenminimierung und Zweckbindung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

G. CNIL Recommendations, (I.) Sheet 2

„The purpose of the processing is the aim of the use of personal data. This objective must be specified, i.e. defined as soon as the project starts. It must also be explicit, that is to say, known and understandable. Finally, it must be legitimate, i.e. compatible with the tasks of the organisation."

„The data must not be further processed in a manner incompatible with this initial purpose: the principle of purpose limitation restricts how the controller may use or reuse these data in the future."

# 2. Datenminimierung und Zweckbindung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

## G. CNIL Recommendations, (II.) Sheet 2

„[General purpose AI systems and foundation models] […] can be used for a wide variety of applications and for which it may be difficult to define a sufficiently specified and explicit purpose at the development stage." „The purpose of the processing during the development stage may be considered to be specified, explicit and legitimate only if it is sufficiently specific, i.e. **where it refers cumulatively to:**

**the 'type' of system developed**, such as, for example, the development of a large language model (LLM), a computer vision system or a generative AI system for images, videos or sounds. The types of systems must be presented in a sufficiently clear and intelligible way for the data subjects [...].

**technically feasible functionalities and capabilities**, which means that the controller must draw up a list of capabilities that he or she can reasonably foresee at the development stage."

**„Examples of purposes considered to be explicit and specified:**
Development of a large language model (LLM) able to answer questions, generate text according to context (emails, letters, reports, including computer code), perform translations, summaries [...] etc.;
[...]"

# 3. PERSONENBEZUG

# Personenbezug: Art. 4 Nr. 1 DSGVO, ErwG 26

Art. 4 Nr. 1: „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

> ErwG 26, Satz 3Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. 4Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.5

# 3. Personenbezug

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

C. DSK Orientierungshilfe, Rn. 4ff, 7f, 48 ff.

Allerdings ist hierbei zu beachten, dass ein Personenbezug sich durch viele Merkmale, nicht nur durch Namen und Adressdaten ergeben kann. Die Prüfung, ob personenbezogene Daten in einem Einsatzfeld vorkommen oder nicht, ist daher gründlich und über den Lebenszyklus der Daten hinweg durchzuführen.

Trainingsphase: Rn. 7f

Personenbezug bei Nutzung des KI Systems (Eingabe Prompt) Rn. 48ff.

# 3. Personenbezug

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

D. Rechtsgrundlagen LFDI BaWü, S. 6, 7

Inwieweit KI-Systeme personenbezogene Daten verarbeiten, ist abhängig vom Zeitpunkt der Bewertung: Es kann von vornherein eine Identifizierbarkeit der natürlichen Personen wahrscheinlich sein oder erst zu einem späteren Zeitpunkt mit Zusatzinformationen. Es sind jeweils die zum Einsatz gelangenden maschinellen Lernverfahren ebenso zu analysieren wie die Wahrscheinlichkeit, dass eine (Re)Identifizierbarkeit natürlicher Personen durch atypisches Einwirken auf die Systeme möglich ist.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 3. Personenbezug

Spezifisch zum Personenbezug in LLM vgl. Hamburger Thesen v. 15.7.2024

1. Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Denn in LLMs werden keine personenbezogenen Daten gespeichert. Soweit in einem LLM-gestützten KI-System personenbezogene Daten verarbeitet werden, müssen die Verarbeitungsvorgänge den Anforderungen der DSGVO entsprechen. Dies gilt insbesondere für den Output eines solchen KI-Systems.

2. Mangels Speicherung personenbezogener Daten im LLM können die Betroffenenrechte der DSGVO nicht das Modell selbst zum Gegenstand haben. Ansprüche auf Auskunft, Löschung oder Berichtigung können sich jedoch zumindest auf Input und Output eines KISystems der verantwortlichen Anbieter:in oder Betreiber:in beziehen.

3. Das Training von LLMs mit personenbezogenen Daten muss datenschutzkonform erfolgen. Dabei sind auch die Betroffenenrechte zu beachten. Ein ggf. datenschutzwidriges Training wirkt sich aber nicht auf die Rechtmäßigkeit des Einsatzes eines solchen Modells in einem KI-System aus.

# 3. Personenbezug

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

G. CNIL Recommendations, Introduction

In practice, three cases may be encountered:

**It is certain that no personal data is present in the dataset**: the how-to sheets [#GDPR] are not applicable (although some recommendations may be relevant as good practices).

**It is certain that personal data are present:** the how-to sheets [#GDPR] apply. This is the case for AI systems developed from videos or images of people, voice recordings, structured personal data, etc. It should be noted that the European texts lay down the rule that 'mixed' datasets are governed by the GDPR, if both types of data are inextricably linked.

**Personal data may be present**: this is a frequent case for which the collection of personal data is not expressly desired. For example:

- residual presence of persons or license plates in images;
- occurrences of surnames, first names, addresses, etc. in textual data such as comments or prompts, etc.

In the latter case, the how-to sheets apply. However, verification operations may be carried out as a result of the collection in order to delete the remaining personal data. This can be achieved:
by manual verification, e.g. when annotating the data;
by automatic verification, e.g. by using techniques for detecting persons/faces in images, by nameentity recognition methods (NER), etc.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 4. RECHTSGRUNDLAGEN

# 4. Rechtsgrundlagen für die Datenverarbeitung

Art. 5 Abs. 1 lit. a DS-GVO:

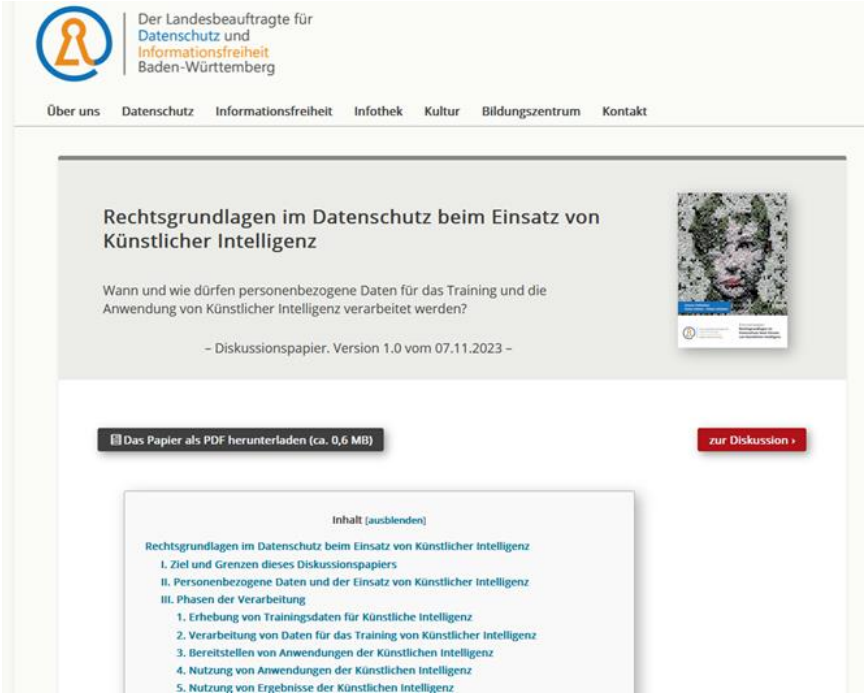
„Personenbezogene Daten müssen auf rechtmäßige Weise […] verarbeitet werden“

EwGr. 40 DS-GVO:

„Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, die sich aus dieser Verordnung oder – wann immer in dieser Verordnung darauf Bezug genommen wird – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt, so unter anderem auf der Grundlage, dass sie zur Erfüllung der rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist.“

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 4. Rechtsgrundlagen für die Datenverarbeitung



# 4. Rechtsgrundlagen für die Datenverarbeitung

**G. CNIL: Recommendations on the development of AI systems**

– Sheet 8

Zum berechtigten Interesse:

„Thus, the following interests could be considered a priori legitimate for the development of AI systems:

- carry out scientific research (in particular for bodies which cannot rely on the public interest mission);
- facilitate public access to certain information;
- develop new systems and functionalities for users of a service;
- offer the service of a conversational agent to assist users;
- improve a product or service to increase its performance;
- develop an AI system to detect fraudulent content or behaviour.
- The commercial purpose of the development of an AI system is not in itself contradictory to the use of the legal basis of legitimate interests.

Conversely, certain interests cannot be regarded as legitimate, in particular where the AI system envisaged has no connection with the mission and activity of the body or where it cannot be lawfully deployed.

[…]

Please note: more generally, the development of systems which are categorically prohibited by regulations other than the GDPR cannot be regarded as legitimate. In this regard, particular attention should be paid to the AI-specific categorisation used in the European AI Act.“

# 4. Rechtsgrundlagen für die Datenverarbeitung

**G. CNIL: Recommendations on the development of AI systems**

– Sheet 8

Zur Erforderlichkeit:

„That means, in particular, that the controller must ensure that it is necessary to process personal data or to store them in a form which permits the direct or indirect identification of individuals, and that it is necessary to have recourse, where appropriate, to a technical solution which involves processing a large volume of personal data."

Zur Interessenabwägung:

„The following factors make it possible to measure the positive impact of the interests pursued:
[...] The diversity of applications implementing AI systems shows that there can be many benefits, such as improved healthcare, better accessibility of certain essential services, facilitation of the exercise of fundamental rights such as access to information, freedom of expression, access to education, etc."

# 4. Rechtsgrundlagen für die Datenverarbeitung

**G. CNIL: Recommendations on the development of AI systems**

– Sheet 8

Zur Interessenabwägung (Fortsetzung):

„The following impacts on people should therefore be considered and the level of associated risks should be assessed in the case at hand. Three types of risks can be distinguished:

1.Impacts on individuals related to the collection of data used to develop the system, in particular where data have been scraped online

- Risks of infringement of privacy and rights guaranteed by the GDPR [...]
- Risks of illegal collection [...]
- Risks of undermining freedom of expression [...]

2. Impacts on individuals related to model training and data retention

- Risks of loss of confidentiality of the data contained in the dataset or in the model [...]
- Risks related to the difficulty of ensuring the effectiveness of the data subject rights [...]
- Risks associated with the difficulty of ensuring transparency towards data subjects [...]

3. Impacts on persons related to the use of the AI system

- Risks of reputational damage, spread of false information or identity theft, where the AI system (particularly generative AI) produces content on an identified or identifiable natural person [...]
- Risks of infringement of certain rights or secrets provided for by law [...]
- Serious ethical risks, which may impact certain general legal principles or the proper functioning of society as a whole, related to the development of certain AI systems. [...]“

# 4. Rechtsgrundlagen für die Datenverarbeitung

**G. CNIL: Recommendations on the development of AI systems**

– Sheet 8

Zur Interessenabwägung (Fortsetzung 2):

„The following measures have been identified as relevant to limit the impact on data subject rights and freedoms. They must be adapted to the risks posed by the different processing of the development phase.

1. In response to the risks associated with the collection and compilation of the dataset:

- Anonymise at short notice or, failing that, pseudonymise the data collected [...]
- Where it does not adversely affect the performance of the model developed, synthetic data should be used [...]

2. In response to risks related to model training and data retention

- Implement technical, legal and organisational measures in addition to the obligations laid down in the GDPR in order to facilitate the exercise of rights [...]“

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 5. (MIT-)VERANTWORTLICHKEIT

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

*Artikel 26*

**Gemeinsam für die Verarbeitung Verantwortliche**

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

*Artikel 28*

**Auftragsverarbeiter**

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

# 5. (Mit-)Verantwortlichkeit

C. DSK Orientierungshilfe, Rn. 32 ff.

Wird die KI-Anwendung von einer Stelle ausschließlich zu eigenen Zwecken auf eigenen Servern betrieben, ist diese Stelle in der Regel auch als alleiniger Verantwortlicher anzusehen.

Setzt eine Stelle zu eigenen Zwecken eine KI-Anwendung eines externen Anbieters zum Beispiel als Cloud-Lösung ein, agiert der externe Anbieter als verlängerter Arm im Auftrag des Verantwortlichen. Dann besteht zwischen dem Anbieter der Anwendung und dem Verantwortlichen häufig ein Auftragsverarbeitungsverhältnis gemäß Art. 28 f. DS-GVO mit der Folge, dass mit dem Anbieter eine Vereinbarung gemäß Art. 28 Abs. 3 DS-GVO abzuschließen ist.

Von einer gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO kann auszugehen sein, wenn zwei Stellen gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden, also eine gemeinschaftliche Entscheidung hierüber treffen. Eine gemeinsame Verantwortlichkeit kann aber auch vorliegen, wenn die beteiligten Stellen sich ergänzende Entscheidungen treffen und diese für die Verarbeitung in einer Weise erforderlich sind, dass sie einen spürbaren Einfluss auf die Bestimmung der Zwecke und Mittel der Verarbeitung nehmen. Ein wichtiges Kriterium für die Annahme einer gemeinsamen Verantwortlichkeit bei konvergierenden Entscheidungen ist insbesondere, ob die Verarbeitung ohne Beteiligung beider Stellen an den Zwecken und Mitteln nicht möglich wäre in dem Sinne, dass die Verarbeitungsvorgänge beider

# 5. (Mit-)Verantwortlichkeit

G. CNIL Recommendations

Examples of controllers:

A video streaming platform wants to develop a recommendation AI system. For this purpose, it reuses a dataset of its customers that was originally collected for the purpose of providing the service.
The streaming platform that creates the training dataset is responsible for this new processing since it has decided on the purpose (train a recommendation AI system) and the essential means of processing (i.e. the dataset it has already collected for another purpose).

The provider of a conversational agent who trains its large language model (LLM) from publicly available data on the Internet is controller of the reuse of publicly available personal data on the Internet. Indeed, the provider decides both the purpose (proposing a conversational agent) and the essential means of processing (selecting the data to be re-used).

A provider develops an AI system based on a pre-trained model with personal data. The provider intends to retrain or adjust the model (through fine-tuning or transfer learning) with a dataset that it set up, at its initiative. In such a case, that provider will have to be classified as a controller, provided that it pursues a purpose of its own and for which it determines itself the essential means.

# 5. (Mit-)Verantwortlichkeit

G. CNIL Recommendations

When the training dataset of an AI system is fed by more than one controller for a jointly defined purpose, the controllers may be qualified as joint controllers.
Examples:

Case 1: academic hospitals developing an AI system for the analysis of medical images choose to use the same federated learning protocol. The latter allows them to exploit data for which they are initially separate controllers, in order to benefit from the mutualization.
Together, they determine the purpose (training a medical imaging AI system) and the means of this processing (through the choice of the protocol and the determination of the data they exploit): they are therefore jointly responsible for this training processing.

Case 2: a consortium consisting of a municipality, a company providing automated image processing software and a company providing video devices is conducting an experiment to install enhanced cameras to record and analyse the flow and behaviour of vehicles using a traffic lane within the municipality. The contract between the city and the two companies provides for the use of the software by the municipality in real-time conditions and the possibility for companies to improve the automated image processing software by the data collected in real time. This improvement of the automated processing software benefits both the municipality and the companies providing automated image processing software and video devices.

The municipality and the two companies would thus be jointly responsible for the processing of the training dataset of the automated image processing software, provided that they jointly decide on the purpose and essential means of the processing and the companies do not act solely on behalf of the municipality. Indeed, it is possible to consider that they jointly decide on the essential means of processing (by choosing to feed the AI system training dataset with real-time data collected by enhanced cameras and data already collected by the company providing the automated image processing software) and the purpose of the processing (experimentally train an AI system that detects particular vehicle behaviour and improves the automated image processing software).

Conversely, if one of the companies intends to reuse the data for its own purpose, which it would be the only one to benefit from (e.g. in a research and development framework), then it could be considered that it is responsible for a separate processing.

# 5. (Mit-)Verantwortlichkeit

G. CNIL Recommendations

An AI system provider may use a provider to collect and process the data according to its documented instructions (e.g. to collect publicly available data on the Internet, reuse a specific dataset made available online, etc.). The latter then qualifies as a processor. It is essential for the provider of the AI system, as the controller, to ensure that its processor complies with the GDPR and limits the processing of data to its instructions, in particular by concluding a data processing agreement.

Moreover, the fact of using the same dataset for several customers, in the context of separate services, is generally a decisive indication that the provider is responsible for a separate processing, at least for the establishment of the database.

Example:

A provider has been entrusted with the creation of a training dataset by an AI system provider who has indicated precisely how it should be developed (in particular with regard to data sources and categories, with quality and documentation requirements). This service provider is likely to act as a processor.

Conversely, a service provider which, on its own initiative, would have created a dataset which it operates by developing AI systems adapted to the needs of each of its customers will likely be responsible for the processing of this dataset, regardless of its role in the specific processing carried out for those customers (which it could implement as a processor, for example on the basis of data provided by the customers themselves).

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 6. TRANSPARENZGEBOT UND INFORMATIONSPFLICHTEN

## 6. Transparenzgebot und Informationspflichten

Artikel 5 Abs. 1 lit. a) Personenbezogene Daten müssen

auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)

Artikel 12 Abs. 1:

Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.

# 6. Transparenzgebot und Informationspflichten

C. DSK Orientierungshilfe (I) ,Rn. 21ff.

Im Allgemeinen (Punkt 1.8):

> „Sofern Verantwortliche eine KI-Anwendung nicht selbst entwickeln, müssen sie darauf achten, dass Ihnen vom Anbieter ausreichend Informationen zur Verfügung gestellt werden, um die Transparenzanforderungen der Art. 12 ff. DS-GVO umsetzen zu können. Dafür haben die Hersteller den KI-Anwendern entsprechende Dokumentationen bereitzustellen. Wird die KI-Anwendung zum Beispiel als Cloud-Lösung eingesetzt, ist der Auftragsverarbeiter gemäß Art. 28 Abs. 3 Satz 2 lit. e DS-GVO verpflichtet, den Verantwortlichen dabei zu unterstützen, den Rechten der betroffenen Person nachzukommen.“
>
> „Zu den Informationen, über die die Verantwortlichen informieren und Auskunft erteilen müssen, zählen auch Angaben über die bei einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 DS-GVO involvierte Logiksowie die Tragweite und die möglichen Auswirkungen für die betroffene Person. Der Begriff der automatisierten Entscheidung wird viele KI-Anwendungen erfassen, die selbst automatisiert Entscheidungen treffen oder deren Ergebnis Entscheidungen wesentlich beeinflusst.“
>
> „Aus dem Begriff der „Logik“ lässt sich dabei mindestens schließen, dass eine Erläuterung der Methode der Datenverarbeitung bezogen auf die Funktionsweise des Programmablaufs im Zusammenhang mit der konkreten Anwendung vorzunehmen ist. Visualisierungen und interaktive Techniken können dabei helfen, die Komplexität der Logik auf ein verständliches Maß herunter zu brechen.“

# 6. Transparenzgebot und Informationspflichten

D. Rechtsgrundlagen LFDI BaWü S. 12

„Eine weitere Schwierigkeit kann die Intransparenz und mangelnde Nachvollziehbarkeit komplexer KI-Systeme sein, wenn dadurch die Einhaltung der datenschutzrechtlichen Anforderungen in Form einer hinreichend bestimmten und informierten Einwilligungserklärung infrage zu stellen ist. Die Informationen müssen in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache sein, dass die betroffene Person die Funktionsweise der Datenverarbeitung verstehen kann.Dem nachzukommen kann für Verantwortliche insbesondere dann herausfordernd sein, wenn sogar Fachleute die KI-Systeme und deren Datenverarbeitungsprozesse aufgrund ihrer Komplexität und Architektur (z. B. bei der Verwendung von tiefen neuronalen Netzen) nicht mehr eindeutig nachvollziehen können."

„Der Intransparenz und mangelnden Nachvollziehbarkeit kann jedoch bis zu einem gewissen Grad entgegengewirkt werden, indem der betroffenen Person zumindest die Informationen über die wesentlichen Aspekte der Datenverarbeitung – wie etwa Informationen über die Zwecke der Datenverarbeitung sowie die Person des Verantwortlichen – bereitgestellt werden (z. B. in den Datenschutzhinweisen)."

Leitfragen:

> „Liegt eine informierte, eindeutig bestätigende Einwilligungserklärung […] vor?"
>
> „[…] Kann die betroffene Person bei der Verwendung des (komplexen) KI-Systems überhaupt so informiert sein, dass sie abschätzen kann, welche Auswirkungen und Tragweite die Datenverarbeitung hat?"

# 6. Transparenzgebot und Informationspflichten

H. FAQ KI und Datenschutz DSB Österreich

„Bei der Verarbeitung nach Treu und Glauben handelt es sich um einen übergreifenden Grundsatz, der verlangt, dass personenbezogene Daten nicht in einer Weise verarbeitet werden dürfen, die für die betroffene Person ungerechtfertigt nachteilig, diskriminierend, unerwartet oder irreführend ist. Insbesondere darf es nicht zu einer Übertragung des Risikos vom Verantwortlichen auf die betroffene Person – etwa durch einen Hinweis in den AGB – kommen.“

„Der Grundsatz der Transparenz steht damit stark in Verbindung und verlangt, die betroffene Person entsprechend über die Verarbeitung ihrer personenbezogenen Daten zu informieren (siehe dazu auch den Punkt „Betroffenenrechte“).“

*„Beispiel:*
*Auf einer Versicherungs-Website wird ein „intelligenter Chatbot“ für den Kundenservice verwendet, bei welchem Kund:innen in ihren Anfragen auch regelmäßig personenbezogene Daten preisgeben. Es muss sichergestellt werden, dass die Kund:innentransparent darüber informiert werden, wie genau eingegebene personenbezogene Daten verarbeitet werden. Die Interaktion mit dem Chatbot hat für die betroffene Person zudem keine unvorhergesehenen oder nachteiligen Folgen.“*

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 7. AUSKUNFTSANSPRUCH UND RECHT AUF LÖSCHUNG

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 7. Auskunftsanspruch und Recht auf Löschung

C. DSK Orientierungshilfe, Rn. 26, 28 ff.

„Verantwortliche müssen gewährleisten, dass betroffene Personen ihre Rechte auf Berichtigung gemäß Art. 16 DS-GVO und Löschung gemäß Art. 17 DS-GVO ausüben können. Für beide Rechte müssen organisatorische und technische Verfahren konzipiert werden, damit diese auch wirksam ausgeübt werden können. Dafür sind die Vorgaben der datenschutzkonformen Technikgestaltung umzusetzen."

„Machen betroffene Personen von ihrem Recht auf Löschung gemäß Art. 17 Abs. 1 DS-GVOGebrauch, ist zu beachten, dass einige KI-Anwendungen gegebenenfalls durch die Verknüpfung unterschiedlicher Daten einen Personenbezug herstellen können. Es ist daher besonders wichtig, dass bei der Löschung personenbezogener Daten darauf geachtet wird, dass eine Wiederherstellung des Personenbezugs dauerhaft unmöglich ist. Dies kann je nach KI-Anwendung auf verschiedenen Wegen umgesetzt werden."

„Das Unterdrücken von unerwünschten Ausgaben mittels nachgeschalteter Filter stellt zwar nicht generell eine Löschung im Sinne von Art. 17 DS-GVO dar. Denn die Daten, die nach einer bestimmten Eingabe zu einer bestimmten Ausgabe führen, könnten weiterhin personenbeziehbar für das KI-Modell verfügbar sein. Filtertechnologien können aber einen Beitrag dazu leisten, bestimmte Ausgaben zu vermeiden und damit den Rechten und Freiheiten der von einer bestimmten Ausgabe betroffenen Personen dienen."

# 7. Auskunftsanspruch und Recht auf Löschung

D. Rechtsgrundlagen LFDI BaWü S. 12

„Macht die betroffene Person von ihrem Widerrufsrecht Gebrauch, so hat der Verantwortliche gemäß Art. 17 Abs. 1 Buchst. b DS-GVO ihre personenbezogenen Daten unverzüglich zu löschen, sofern es an einer anderweitigen Rechtsgrundlage für die Datenverarbeitung fehlt.Das könnte unter Umständen Auswirkungen für die Funktionsfähigkeit des KI-Systems haben, wenn dieses auf Grundlage eben dieser Daten trainiert wurde oder eine Separierung der betroffenen Datensätze zur Erfüllung der Löschungspflicht mit einem unverhältnismäßigem Aufwand umsetzbar wäre.“

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 7. Auskunftsanspruch und Recht auf Löschung

E. Checkliste (I) BayLDA, S. 5, 6, 10

Bei der Erstellung und beim Einsatz von KI-Modellen muss…

> ... sichergestellt werden, dass Auskunftsersuchen nach Art. 15 DS-GVO auch bei Anfragen zum Training in KI-Modellenim Datenschutzmanagement berücksichtigt werden.
>
> …bei konkretem Auskunftsersuchen nach Art. 15 DS-GVO in Bezug auf ein personenbeziehbares KI-Modell – je nach KI-Technologie – geprüft werden, ob personenbezogene Daten im KI-Modell direkt ermittelbar sind oder ob diese evtl. nur mit Zusatzinformationen (z. B. konkreter Prompt bei GroßemSprachmodell) auf einem KI-Modell abgeleitet werden können. Diese Zusatzinformationen sind im Zweifel vom Betroffenen dann anzufordern.
>
> … sichergestellt werden, dass Betroffenenrechte zur Berichtigung nach Art. 16 DS-GVO, zur Löschung nach Art. 17 DS-GVO, nach Einschränkung der Verarbeitung nach Art. 18 DS-GVO, nach Datenübertragbarkeitnach Art. 20 DS-GVO und des Widerspruchs nach Art. 21 DS-GVO in Bezug auf KI auch im Datenschutzmanagement berücksichtigt werden. Rückmeldefristen an Antragsteller sind hierbei zu beachten.
>
> … bei einem Löschersuchen nach Art. 17 DS-GVO in Bezug auf ein personenbeziehbares KI-Modell – je nach KI-Technologie – geprüft werden, ob personenbezogene Daten im KI-Modell direkt ermittelbarsind oder ob diese evtl. nur mit Zusatzinformationen (z. B. konkreter Prompt bei Großem Sprachmodell) aus einem KI-Modell abgeleitet werden können. Sofern eine Löschung in einem KI-Modell technisch ohne Beeinträchtigung des Gesamtmodells möglich ist, ist der Löschvorgang auch durchzuführen. Sollten andererseits personenbezogene Daten nur mittels Zusatzinformationen(z. B. Prompts) aus einem KI-Modell ermittelbar sein, dann besteht eine Möglichkeit des technischen Löschens darin, mittels Nachtraining die spezifisch zu löschende personenbezogene KI-Ausgabe mittels Anpassung der internen (Wahrscheinlichkeits-)Parameter umzusetzen

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 8. Automatisierte Entscheidung und Profiling

# 8. Automatisierte Entscheidungen und Profiling

C. DSK OH KI, Rn. 12 ff.

Entscheidungen mit Rechtswirkung dürfen gemäß Art. 22 Abs. 1 DS-GVO grundsätzlich nur von Menschen getroffen werden. Ausnahmen sind nur in bestimmten Fällen zugelassen, etwa bei einer Einwilligung der betroffenen Person. Erarbeitet eine KI-Anwendung Vorschläge, die für eine betroffene Person Rechtswirkung entfalten, muss das Verfahren so gestaltet werden, dass dem entscheidenden Menschen ein tatsächlicher Entscheidungsspielraum zukommt und nicht maßgeblich aufgrund des KI-Vorschlags entschieden wird. Unzureichende Personalressourcen, Zeitdruck und fehlende Transparenz über den Entscheidungsweg der KI-gestützten Vorarbeit dürfen nicht dazu führen, dass Ergebnisse ungeprüft übernommen werden. Eine lediglich formelle Beteiligung eines Menschen im Entscheidungsprozess ist nicht ausreichend.

Beispiel:

Eine KI-Anwendung wertet alle eingegangenen Bewerbungen auf eine ausgeschriebene Stelle aus und verschickt selbstständig die Einladungen zu den Vorstellungsgesprächen. Dies stellt einen Verstoß gegen Art. 22 Abs. 1 DS-GVO dar.

Bei öffentlichen Stellen gilt außerdem Folgendes: Der vollständig automatisierte Erlass eines Verwaltungsaktes ist in § 35a VwVfG geregelt. Liegen die Voraussetzungen vor, gilt Art. 22 Abs. 1 DS-GVO gemäß Art. 22 Abs. 2 lit. b DS-GVO nicht. Ein vollständig automatisierter Erlass eines Verwaltungsakts ist nur dann zulässig, wenn es sich um eine gebundene Entscheidung handelt und eine ausdrückliche Ermächtigungsgrundlage besteht. Sofern die öffentliche Stelle über einen Beurteilungsspielraum verfügt oder Ermessen ausübt, scheidet der vollständig automatisierte Erlass aus

## 8. Automatisierte Entscheidungen und Profiling

F. Checkliste Hamburg, Ziffer 12

Entscheidungen mit Rechtswirkung sollten grundsätzlich nur von Menschen getroffen werden. Andernfalls sind die Voraussetzungen des Art. 22 DSGVO zu beachten. Erarbeitet ein LLM-basierter Chatbot Vorschläge, die durch Beschäftigte angenommen werden, müssen diejenigen darauf achten, dass ihnen ein tatsächlicher Entscheidungsspielraum zukommt. Vermeiden Sie es, aufgrund der fehlenden Transparenz der KI-gestützten Vorarbeit faktisch an die Vorschläge gebunden zu sein, weil Sie den Entscheidungsweg nicht nachvollziehen können.

# 8. Automatisierte Entscheidungen und Profiling

H. DSB Österreich

Von Art. 22 DSGVO erfasst sind daher nicht sämtliche automatisierten Entscheidungen, sondern nur solche, die sich besonders auf die Rechtsposition von betroffenen Personen auswirken. In Erwägungsgrund 71 DSGVO werden als Beispiele für solch automatisierte Entscheidungen die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen genannt.

Dies gilt nur in drei Fällen nicht:
Die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrags zwischen der Person und dem Verantwortlichen unbedingt erforderlich,
es gibt eine gesetzliche Grundlage und diese enthält angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten und der berechtigten Interessen der betroffenen Person oder
die Person hat ihre ausdrückliche Einwilligung erteilt.

Auch in diesen Fällen muss die betroffene Person darüber informiert werden, dass eine automatisierte Entscheidung über sie getroffen wird, inklusive der zugrundeliegenden Logik und der angestrebten Auswirkungen der Entscheidung.

Die betroffene Person hat – außer es liegt eine gesetzliche Grundlage vor – zudem das Recht, die Entscheidung anzufechten und ihren Standpunkt darzulegen sowie eine menschliche Intervention zur Überprüfung der Entscheidung zu verlangen.

Soweit automatisierte Entscheidungen auf sensiblen Daten gemäß Art. 9 Abs. 1 DSGVO beruhen, sind darüber hinaus die besonderen Vorgaben von Art. 22 Abs. 4 DSGVO zu beachten.

Beispiel:
Für die Bearbeitung von Bewerbungen wird ein KI-System verwendet, mit dem einige Bewerbungen bei Vorliegen bestimmter Kriterien automatisch aussortiert werden. Da eine automatische Nichtberücksichtigung im Bewerbungsprozess eine rechtliche Wirkung entfaltet bzw. erhebliche Beeinträchtigung darstellen kann, wären die Vorgaben des Art. 22 DSGVO zu prüfen.

Ein Verstoß gegen die Vorgaben von Art. 22 DSGVO kann auch dazu führen, dass das KI-System, welches für die jeweiligen automatisierten Entscheidungen eingesetzt wurde, in dieser Form nicht weiterverwendet werden darf.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 9. DATENSCHUTZ DURCH TECHNIKGESTALTUNG

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 9. Datenschutz durch Technikgestaltung

D. Rechtsgrundlagen LFDI BW, S. 7

Bei der Betrachtung muss indes auch berücksichtigt werden, ob solche Model Attacks nach allgemeinen Ermessen wahrscheinlich sind. Es bedarf damit grundsätzlich einer regelmäßigen Risikobewertung. Diese hat neben der rechtlichen Bewertung der (Re-) Identifizierbarkeit natürlicher Personen, die technischen Methoden im Sinne einer datenschutzkonformen Technikgestaltung einzubeziehen, vgl. Art. 25 Abs. 1 DS-GVO.

Dazu gehören präventive Maßnahmen in der technischen Gestaltung eines KI-Systems derart, dass z. B. Model Attacks vermieden werden, wofür die Methode „Differential Privacy“ diskutiert wird. Ebenso könnte die technische Methoden des „Unlearning“ für das Löschen und das Recht auf Vergessen herangezogen werden, vgl. Art. 17 DS-GVO.

S. 18 (Darstellung Art. 6 I lit. F, Fn 57: „Ebenso kann sich auf die Abwägung auswirken, inwieweit die verantwortliche Stelle Vorgaben von „Data Protection by Design“ und „Data Protection by Default“ umgesetzt hat.

# 9. Datenschutz durch Technikgestaltung

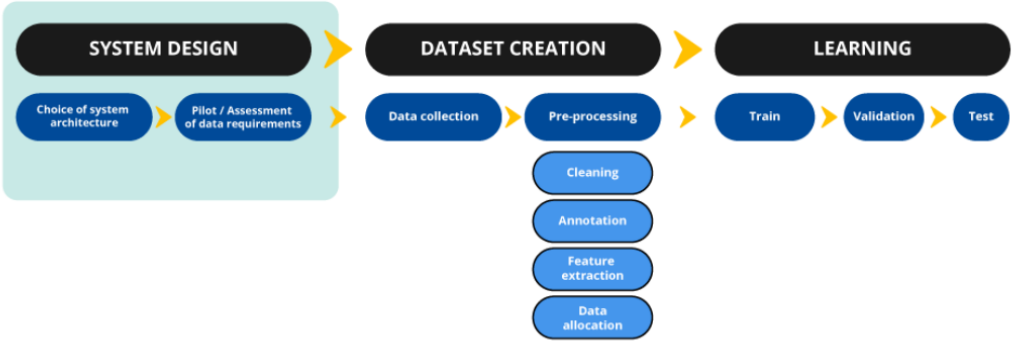
- E CNIL [***]

Sheet 6, 7

Ausführlich und prozessorientiert

When considering the design choices of an AI system, the principles of data protection, and in particular the minimisation principle, must be respected. This approach takes place at four levels. A controller must therefore ask itself about:

- **the objective of the system** it wishes to develop;
- **the method to be used** which will affect the characteristics of the dataset;
- **the data sources mobilized** (see the how-to sheet on the compliance of the processing with the law, on open sources, on third parties, etc.) and among these sources, **the selection of data strictly necessary**, in view of the usefulness of the data and the potential impact their collection has on the rights and freedoms of data subjects;
- **the validity of the choices** previously made. Such validation may take different (non-exclusive) forms, such as a **pilot study** or the solicitation of an ethics committee.



Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# 10. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

## 10. Datenschutz-Folgenabschätzung

C. DSK OH Rn. 38ff

Vor der Verarbeitung personenbezogener Daten ist eine generelle Bewertung (Vorabprüfung) des Risikos hinsichtlich der Art, des Umfangs, des Zwecks und der Umstände der Verarbeitung vorzunehmen.

Soweit der Verantwortliche nicht gleichzeitig Anbieter des KI-Systems ist, ist er zur Durchführung einer Risikobewertung bzw. einer DSFA auf Informationen des Anbietenden insbesondere zur Funktionsweise des Systems angewiesen. Daher ist bei der Auswahl und dem Erwerb eine KI-Anwendung darauf zu achten, dass diese Informationen vom Anbietenden bereitgestellt werden.

# 10. Datenschutz-Folgenabschätzung

G. CNIL, Sheet 5 (umfangreich, Fokus auf ‚AI Risks to consider in a DPIA')

the risks to data subjects related to misuse of the data contained in the training dataset, in particular in the event of a data breach;

the risk of automated discrimination caused by the AI system introduced during development, for example linked to a lower performance of the system for certain categories of people;

the risk of producing fictitious content on a real persons, which is particularly important in the case of generative AI systems, and may have consequences for their reputation;

the risk of automated decision-making caused by automation or confirmation. This risk may arise in particular if the necessary explanatory measures are not taken during the development of the solution (such as the use of a trust score, or intermediate information such as saliency map), thus limiting the ability of the agent using the system to verify its performance under real conditions. This risk may also arise when the staff member is unable to take a decision contrary to the outputs of the system without prejudice to them (due to hierarchical pressure, for example);

the risks associated with known attacks specific to AI systems such as attacks by data poisoning, by inserting a backdoor, or by model inversion;

the risks related to the confidentiality of the data that could be extracted from the AI system;

Systemic and serious ethical risks related to the deployment of the system, such as impacts on the democratic functioning of society, or respect of fundamental rights (e.g. in cases of discrimination), which can be taken into account during the development phase.

Finally, the risk of users losing control over their published online and freely accessible data, as large-scale collection is often necessary for training an AI system, in particular when it is collected by web scraping;

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

# Vielen Dank für Ihre Aufmerksamkeit

Hier Untertitel eintragen