EU Privacy & Security Law

Niko Härting
Partner and Founder of
HÄRTING Rechtsanwälte

Privacy+
Security
Forum

Speakers

Niko Härting

Partner and Founder of HÄRTING Rechtsanwälte

Latest case law from the Court of Justice of the European Union (CJEU)

Privacy+ Security Forum

EU Privacy & Security Law

CJUE, January 9, 2025 – C-416/23

Facts:

- An Austrian citizen had submitted **77 complaints** to the Austrian Data Protection Authority (DPA) within 20 months, whereupon the authority limited processing to two complaints per month

Legal reasoning:

- Filing many complaints isn't enough to label them as "excessive"
- Authorities must prove **abusive intent or bad faith**
- Data protection authorities can refuse to act or charge a fee for excessive requests, but must justify their decision as necessary and proportionate

EU Privacy & Security Law

CJUE, February 13, 2025 – C-383/23

Facts:

- The Danish furniture store chain *ILVA A/S*, a subsidiary of the *Lars Larsen Group*, unlawfully stored personal data of at least 350,000 former customers
- The Danish public prosecutor's office requested a **fine based on the turnover of the entire group**

Legal reasoning:

- The term **“undertaking”** under the GDPR is interpreted in line with EU competition law—meaning any entity engaged in economic activity, regardless of legal form
- Fines under the GDPR should be **based on the global turnover of the entire corporate group**

CJUE, February 27, 2025 – C-203/22

Facts:

- An Austrian citizen applied to the City of Vienna for information about the logic and criteria used by *Dun & Bradstreet Austria GmbH* to create his credit score
- The credit agency refused to disclose the information on the grounds that it contained **business secrets** and personal data of third parties

Legal reasoning:

- Companies must clearly explain how automated credit scoring works
- Information must be presented so that **individuals can understand and challenge the scoring decision**
- Authorities must be able to review the balance between privacy and business interests

EU Privacy & Security Law

CJUE, March 13, 2025 – C-247/23

Facts:

- An Iranian national who was recognized as a refugee in Hungary applied to have his gender entry in the Hungarian asylum register corrected from “female” to “male”
- The Hungarian asylum authority **rejected** the application as there was no evidence of gender reassignment surgery

Legal reasoning:

- GDPR grants a **right to rectification** of inaccurate personal data **without** the need for gender reassignment **surgery**
- However, they may request relevant evidence that is reasonably necessary for the correction

CJUE, January 25, 2024 – C-687/21

Facts:

- Customer entered an installment contract with personal data at *MediaMarkt*
- Documents were mistakenly handed over to another customer
- Error was corrected within 30 minutes; **no evidence of misuse**

Legal reasoning:

- GDPR breach alone does not justify compensation — actual non-material damage required
- Only a **well-founded fear of misuse can lead to damages**
- Article 82 GDPR provides compensation, not punishment

EU Privacy & Security Law

CJUE, April 11, 2024 – C-741/21

Facts:

- The claimant objected to the use of his personal data by juris GmbH for direct marketing
- Despite this, he continued to receive promotional materials
- He sued for compensation under Article 82 GDPR for non-material damage

Legal reasoning:

- The **controller cannot avoid liability** by attributing the fault to an employee or agent
- The criteria from Article 83 GDPR for setting fines should not be applied when determining compensation
- Multiple infringements in the same processing operation should not affect the amount of compensation

EU Privacy & Security Law

Privacy+ Security Forum

CJUE, June 20, 2024 – C-182/22

Facts:

- Plaintiffs' personal data, including sensitive information, were stolen from a trading platform
- **No evidence** indicated that the stolen data were **misused** for fraudulent purposes

Legal reasoning:

- Under Article 82(1) GDPR, compensation is purely compensatory, not punitive
- Non-material damage claims do **not require a minimum severity threshold**
- Minimal compensation is permissible if it fully addresses the damage suffered

CJUE, June 20, 2024 – C-590/22

Facts:

- A tax consultancy firm mistakenly sent clients' tax returns to an outdated address
- It was unclear whether unauthorized individuals accessed the documents

Legal reasoning:

- A GDPR infringement alone does not entitle one to compensation; actual damage must be proven
- Fear of potential data misuse can constitute non-material damage if it leads to demonstrable negative consequences
- Compensation under Article 82 GDPR is not intended to be punitive
- **Violations of national laws do not influence compensation** under Article 82 GDPR

CJUE, May 4, 2023 – C-487/21

Facts:

- The claimant requested a complete copy of his personal data from *CRIF GmbH*, a credit reporting agency, under Article 15(3) GDPR
- *CRIF* provided only a summarized overview
- The claimant demanded the release of full documents, including emails and database extracts

Legal reasoning:

- A **"copy" under Article 15(3) GDPR** is a complete and intelligible reproduction of all personal data undergoing processing
- The copy may include extracts from documents or entire documents and database extracts if necessary to enable the data subject to effectively exercise their rights
- The term **"information" in Article 15(3)** sentence 3 GDPR refers exclusively to the personal data of the data subject

CJUE, June 22, 2023 – C-579/21

Facts:

- A former customer and employee of the Finnish bank Pankki S requested access to his personal data under Article 15(1) GDPR
- He sought information about who accessed his data, when, and for what purpose

Legal reasoning:

- **The right of access includes** information about the identity of individuals who have accessed the data subject's personal data, as well as the purposes and dates of such access
- Employees of the controller who process personal data within the scope of their duties and under the authority of the controller are not considered **"recipients" under Article 15(1)(c) GDPR**

CJUE, October 26, 2023 – C-307/22

Facts:

- A patient requested a first copy of his complete medical records from his dentist without charge
- The dentist refused and demanded reimbursement of costs under the German Civil Code (BGB)

Legal reasoning:

- Patients have the right under Article 15(3) GDPR to obtain a **first copy of their personal** data, even if the purpose is not to verify the lawfulness of processing
- The patient is not required to provide a reason for requesting the copy
- The copy must be a complete and intelligible reproduction of all personal data undergoing processing
- National provisions allowing the controller to **charge for the first copy** of medical records are, with minor exceptions, incompatible with the GDPR

LLMs under the GDPR

Privacy+
Security
Forum

Preliminary: what is “personal data”?

Art. 4 No. 1 GDPR: “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier […]”

- CJEU, October 19, 2016 – **C-582/14** (Breyer); (theoretical) legal possibility of establishing a link to a person is sufficient
- CJEU, November 9, 2023 - **C-319/22** (VIN); means that can “reasonably” be used to establish a link to a person
- CJEU, April 26, 2023 - **T-557/20**: relative standard; the decisive factor is whether the “holder” of the information can establish a personal reference by his own means (pending C-413/23)

And transferred to LLM based AI models?

Is training data in the LLM changed in such a way that only anonymized information is "stored" in the parameters?

- Generally no storage of personal data in the individual layers
- Controversial: Is tokenization merely a "modification" of data?

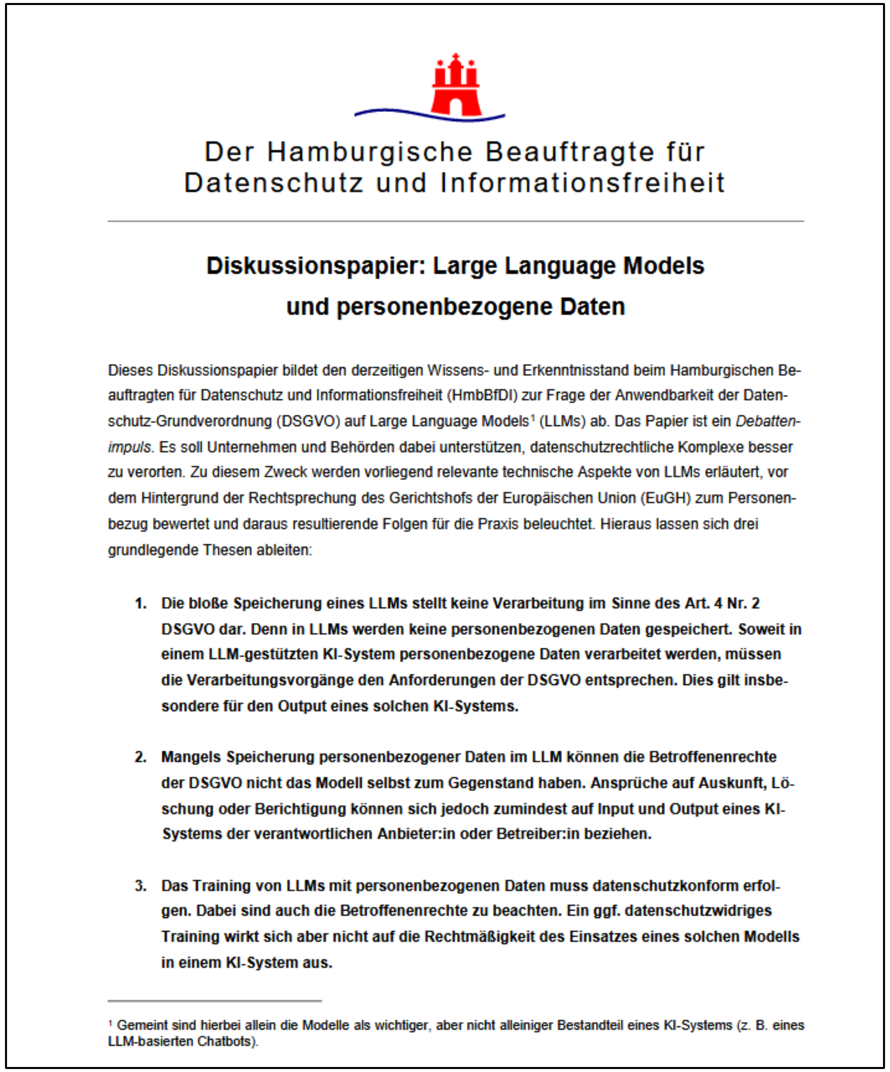
What is the significance of targeted attacks on LLMs ("privacy attacks" or "PII extraction")?

- Able to reproduce training data, which may contain personal data
- But: usually illegal or only possible with a disproportionate effort → data can rather not be qualified as personal in view of Art. 4 No. 1 GDPR and Recital 26 GDPR

And who has to prove all this?

- Very controversial! EDPB: the controller
- But: accountability (Art. 5 para. 2 GDPR) only where personal data is processed.

EU Privacy & Security Law



Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Diskussionspapier: Large Language Models und personenbezogene Daten

Dieses Diskussionspapier bildet den derzeitigen Wissens- und Erkenntnisstand beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) zur Frage der Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) auf Large Language Models[1] (LLMs) ab. Das Papier ist ein *Debattenimpuls*. Es soll Unternehmen und Behörden dabei unterstützen, datenschutzrechtliche Komplexe besser zu verorten. Zu diesem Zweck werden vorliegend relevante technische Aspekte von LLMs erläutert, vor dem Hintergrund der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) zum Personenbezug bewertet und daraus resultierende Folgen für die Praxis beleuchtet. Hieraus lassen sich drei grundlegende Thesen ableiten:

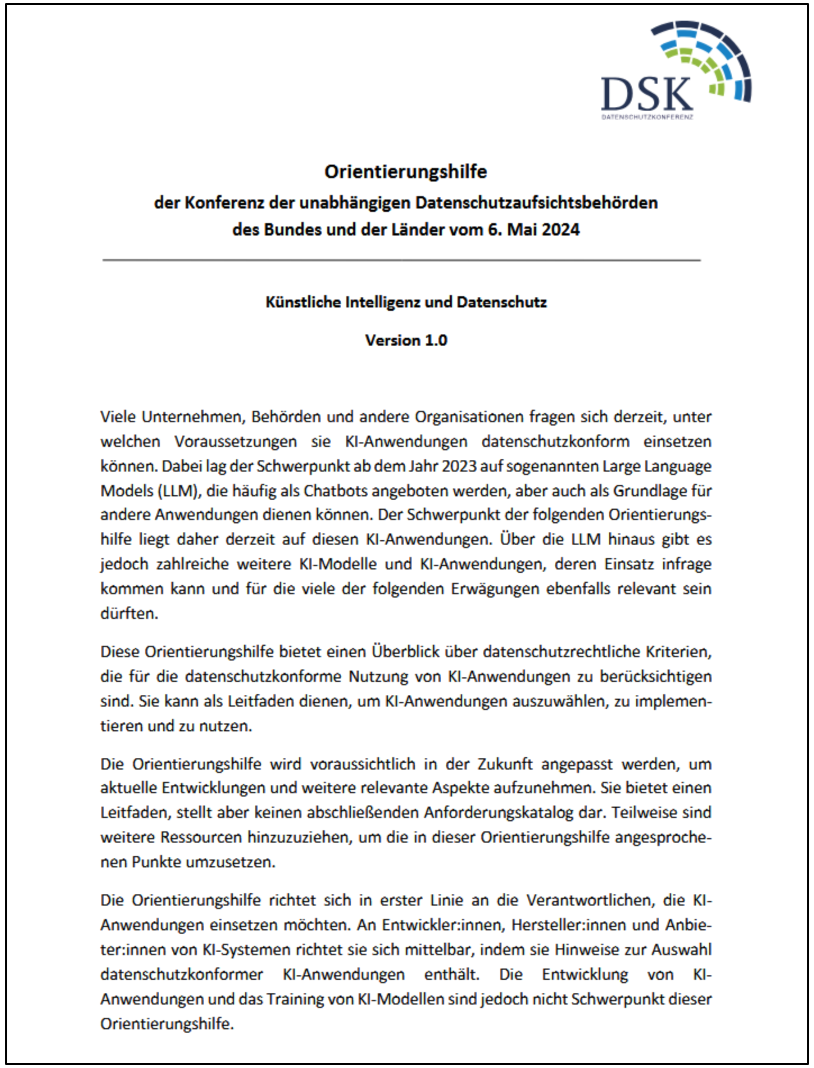
1. **Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Denn in LLMs werden keine personenbezogenen Daten gespeichert. Soweit in einem LLM-gestützten KI-System personenbezogene Daten verarbeitet werden, müssen die Verarbeitungsvorgänge den Anforderungen der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

[1] Gemeint sind hierbei allein die Modelle als wichtiger, aber nicht alleiniger Bestandteil eines KI-Systems (z. B. eines LLM-basierten Chatbots).

EU Privacy & Security Law



DSK
DATENSCHUTZKONFERENZ

Orientierungshilfe
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder vom 6. Mai 2024

Künstliche Intelligenz und Datenschutz

Version 1.0

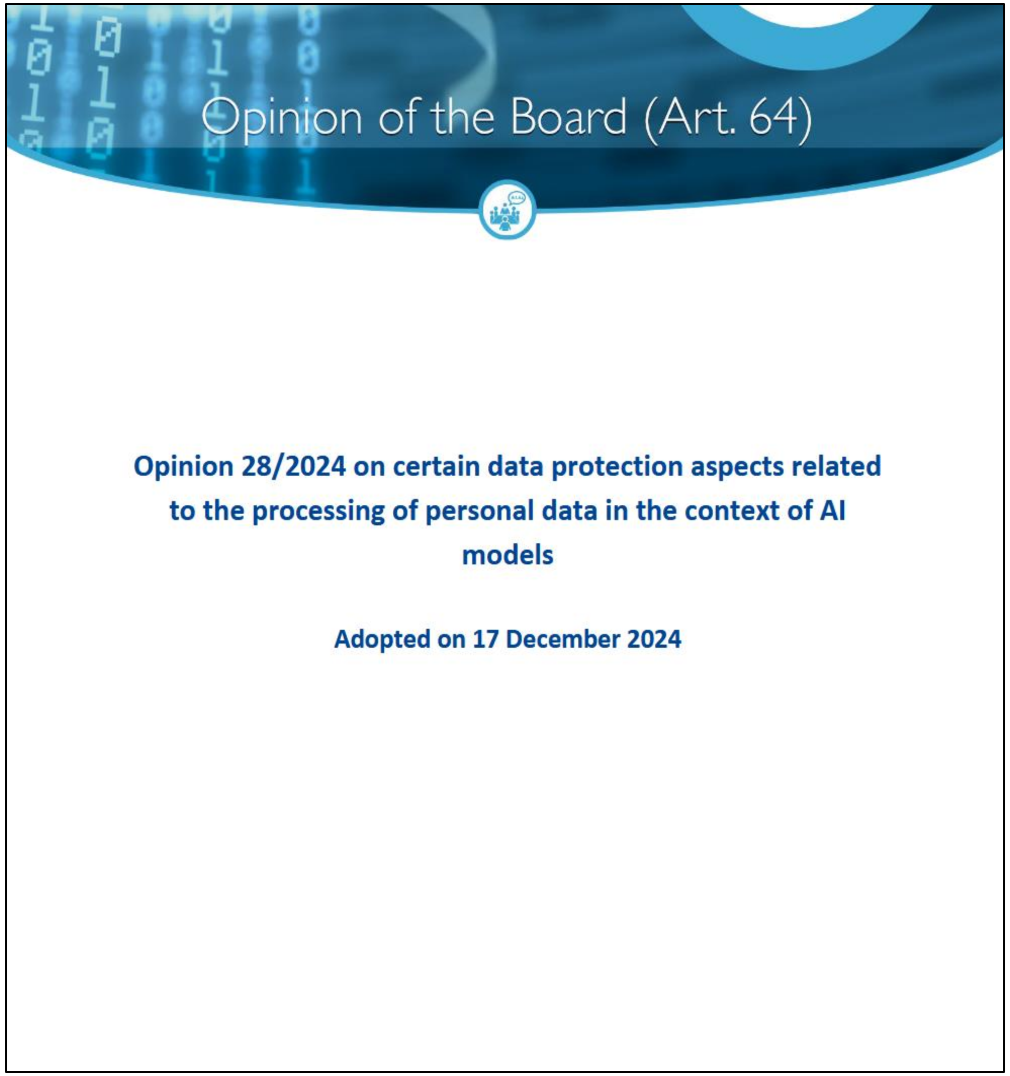
Viele Unternehmen, Behörden und andere Organisationen fragen sich derzeit, unter welchen Voraussetzungen sie KI-Anwendungen datenschutzkonform einsetzen können. Dabei lag der Schwerpunkt ab dem Jahr 2023 auf sogenannten Large Language Models (LLM), die häufig als Chatbots angeboten werden, aber auch als Grundlage für andere Anwendungen dienen können. Der Schwerpunkt der folgenden Orientierungshilfe liegt daher derzeit auf diesen KI-Anwendungen. Über die LLM hinaus gibt es jedoch zahlreiche weitere KI-Modelle und KI-Anwendungen, deren Einsatz infrage kommen kann und für die viele der folgenden Erwägungen ebenfalls relevant sein dürften.

Diese Orientierungshilfe bietet einen Überblick über datenschutzrechtliche Kriterien, die für die datenschutzkonforme Nutzung von KI-Anwendungen zu berücksichtigen sind. Sie kann als Leitfaden dienen, um KI-Anwendungen auszuwählen, zu implementieren und zu nutzen.

Die Orientierungshilfe wird voraussichtlich in der Zukunft angepasst werden, um aktuelle Entwicklungen und weitere relevante Aspekte aufzunehmen. Sie bietet einen Leitfaden, stellt aber keinen abschließenden Anforderungskatalog dar. Teilweise sind weitere Ressourcen hinzuzuziehen, um die in dieser Orientierungshilfe angesprochenen Punkte umzusetzen.

Die Orientierungshilfe richtet sich in erster Linie an die Verantwortlichen, die KI-Anwendungen einsetzen möchten. An Entwickler:innen, Hersteller:innen und Anbieter:innen von KI-Systemen richtet sie sich mittelbar, indem sie Hinweise zur Auswahl datenschutzkonformer KI-Anwendungen enthält. Die Entwicklung von KI-Anwendungen und das Training von KI-Modellen sind jedoch nicht Schwerpunkt dieser Orientierungshilfe.

EU Privacy & Security Law



Opinion of the Board (Art. 64)

Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

Adopted on 17 December 2024

EDPD Opinion of December 17, 2024 – 4 Key Points

1. For an **AI model to be considered anonymous**, both (1.) the likelihood of direct (including probabilistic) extraction of personal data from individuals whose data was used to develop the model and (2.) the likelihood of intentionally or unintentionally obtaining such personal data from queries **must be very low**

2. The **general balancing of interests clause** is in principle a **suitable legal basis** for the processing of personal data both in the context of training and the use of the AI model

EDPD Opinion of December 17, 2024 – 4 Key Points

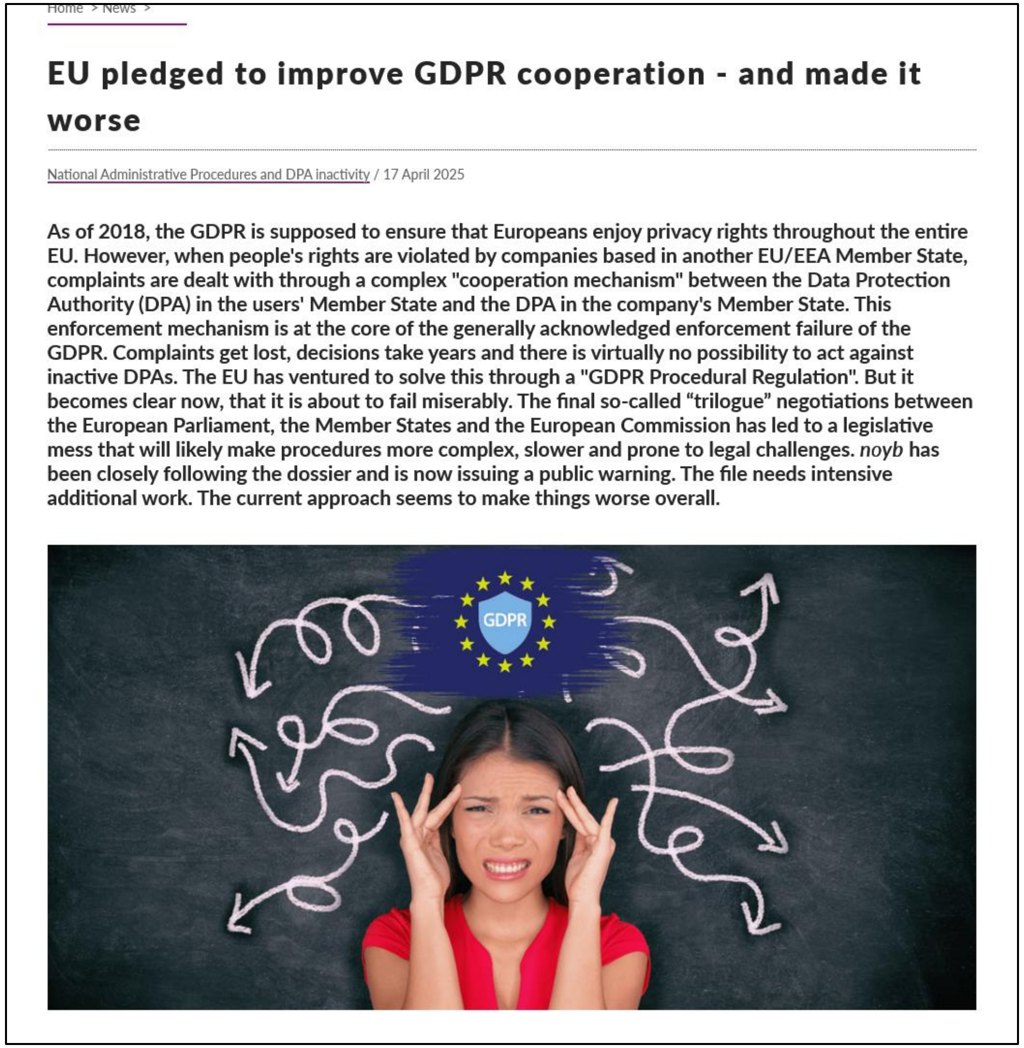
3. If an AI model has been trained in violation of data protection law and personal data can be assumed in the context of the application, the **unlawfulness may (case by case) affect the model**

4. If an AI model has been trained in violation of data protection law, but **no personal reference** can be established in the context of the application, then the AI model is exempt from data protection law (and can be used)

Insights into recent enforcement trends under the GDPR and the upcoming GDPR reform

Privacy+ Security Forum

EU Privacy & Security Law



Home > News >

EU pledged to improve GDPR cooperation - and made it worse

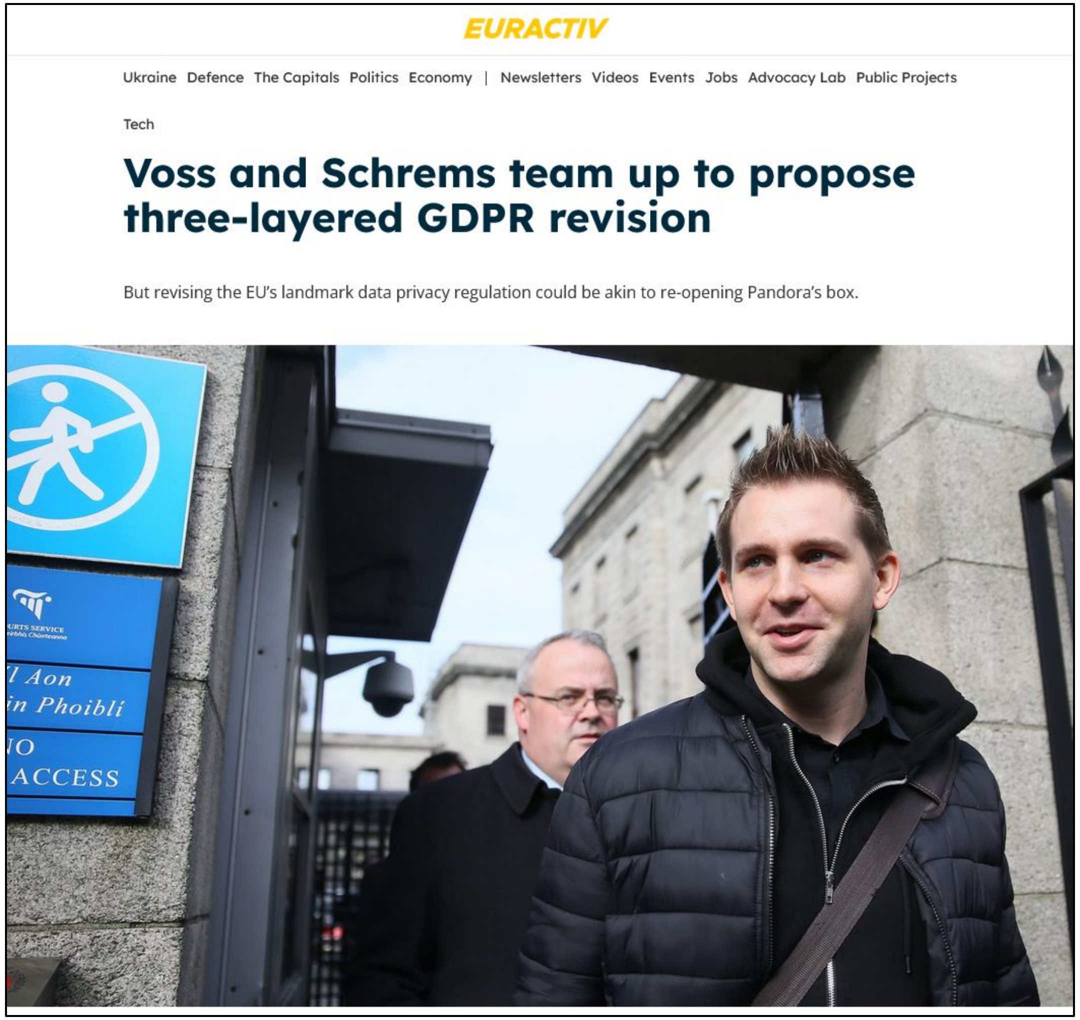
National Administrative Procedures and DPA inactivity / 17 April 2025

As of 2018, the GDPR is supposed to ensure that Europeans enjoy privacy rights throughout the entire EU. However, when people's rights are violated by companies based in another EU/EEA Member State, complaints are dealt with through a complex "cooperation mechanism" between the Data Protection Authority (DPA) in the users' Member State and the DPA in the company's Member State. This enforcement mechanism is at the core of the generally acknowledged enforcement failure of the GDPR. Complaints get lost, decisions take years and there is virtually no possibility to act against inactive DPAs. The EU has ventured to solve this through a "GDPR Procedural Regulation". But it becomes clear now, that it is about to fail miserably. The final so-called “trilogue” negotiations between the European Parliament, the Member States and the European Commission has led to a legislative mess that will likely make procedures more complex, slower and prone to legal challenges. *noyb* has been closely following the dossier and is now issuing a public warning. The file needs intensive additional work. The current approach seems to make things worse overall.

Until 2024: GDPR sacrosanct - no reforms

- **GDPR enforcement across EU borders is failing**, with slow, unclear procedures and little recourse against inactive authorities
- **Only exception: cooperation** between data protection authorities - but not adopted to date

EU Privacy & Security Law



EURACTIV

Ukraine Defence The Capitals Politics Economy | Newsletters Videos Events Jobs Advocacy Lab Public Projects

Tech

Voss and Schrems team up to propose three-layered GDPR revision

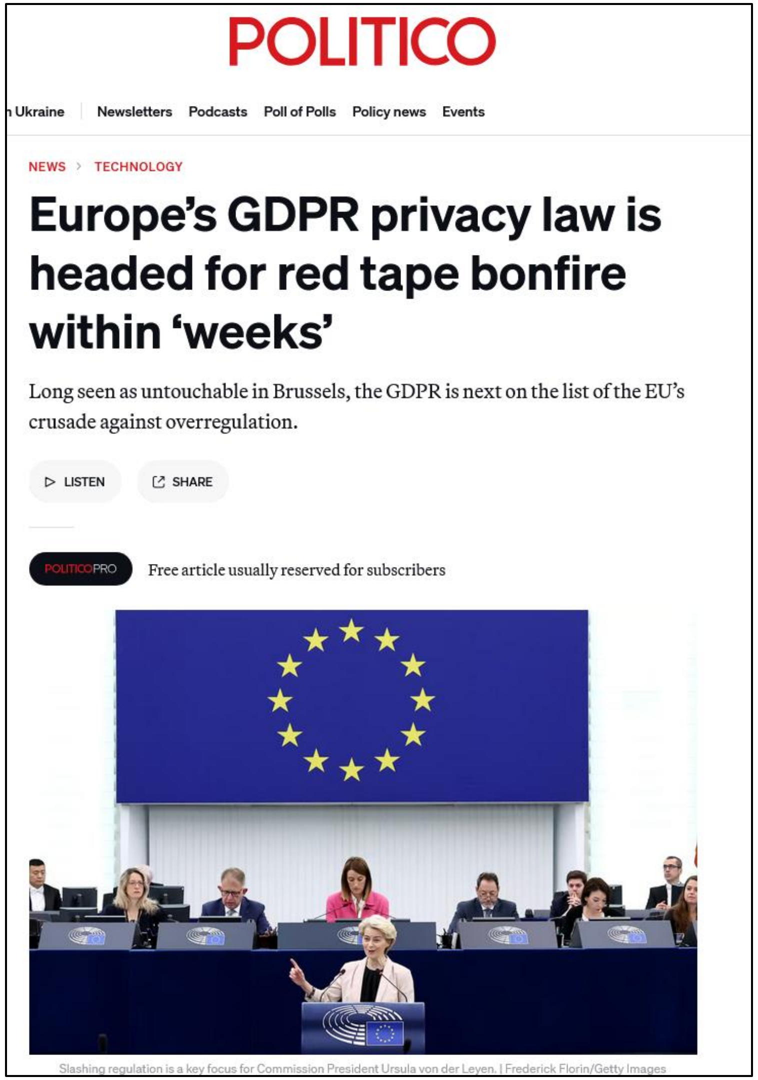
But revising the EU's landmark data privacy regulation could be akin to re-opening Pandora's box.

2024: EP elections and new Commission

- **Axel Voss and Max Schrems propose a three-tier GDPR model** that differentiates obligations based on company size and data use

- **Revising the GDPR risks lobby influence and global impact**, with concerns that reopening it could dilute privacy protections and undermine the EU's role in setting international data standards

EU Privacy & Security Law



POLITICO

n Ukraine | Newsletters | Podcasts | Poll of Polls | Policy news | Events

NEWS > TECHNOLOGY

Europe's GDPR privacy law is headed for red tape bonfire within 'weeks'

Long seen as untouchable in Brussels, the GDPR is next on the list of the EU's crusade against overregulation.

▷ LISTEN | SHARE

POLITICOPRO Free article usually reserved for subscribers

Slashing regulation is a key focus for Commission President Ursula von der Leyen. | Frederick Florin/Getty Images

European Commission and Parliament open to reforms

- **EU plans to simplify the GDPR** to reduce burdens on businesses, especially SMEs, while preserving its core data protection principles
- **Proposed changes** may include easing documentation requirements like record-keeping and data protection impact assessments
- **Risk of intense lobbying** from Big Tech and privacy groups raises concerns that reopening the GDPR could weaken the regulation

EU Privacy & Security Law

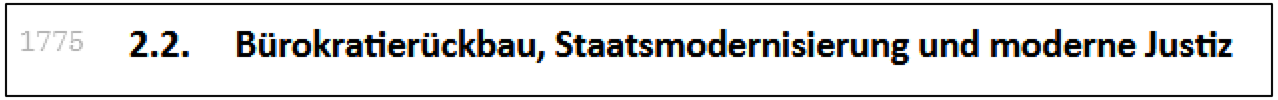
CDU CSU SPD Soziale Politik für Dich.

Verantwortung für Deutschland

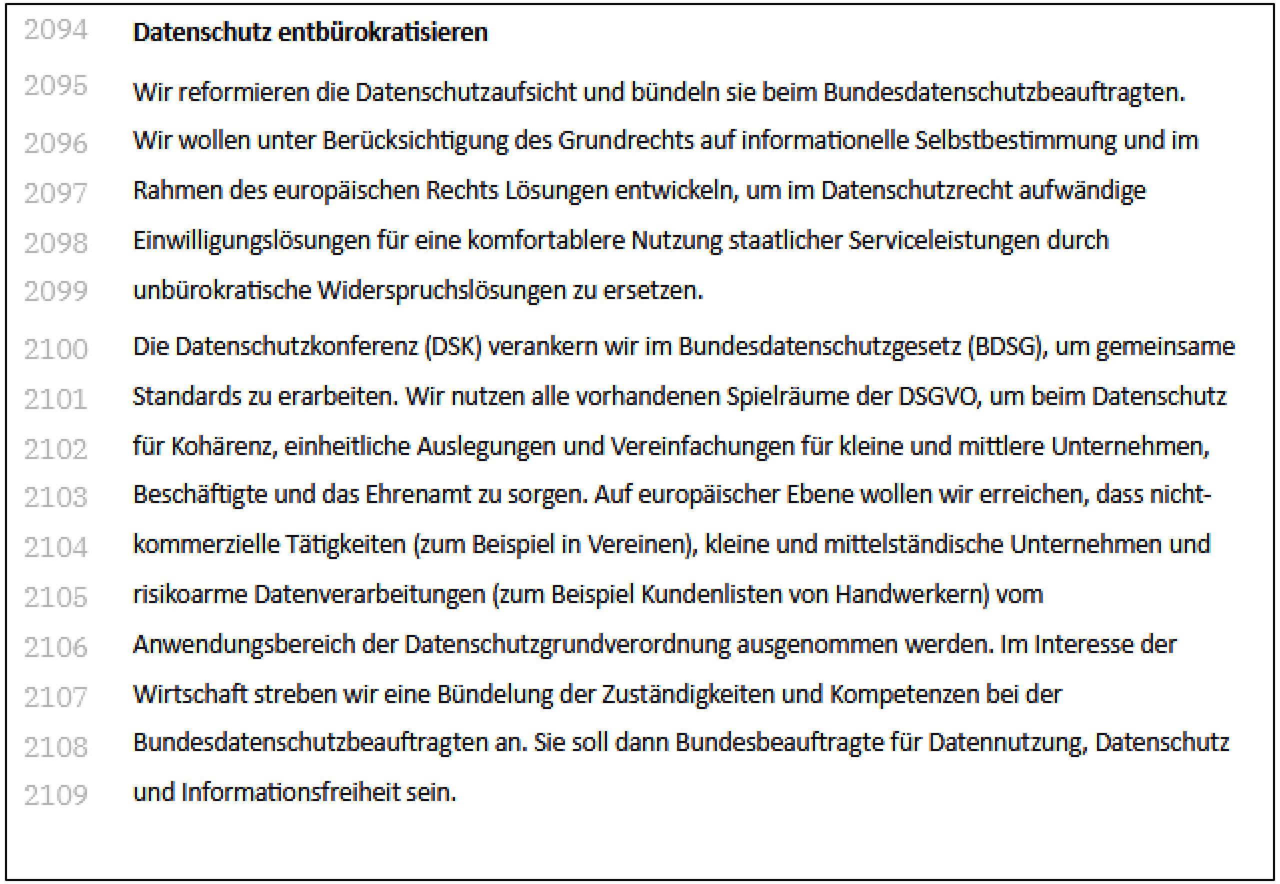
Koalitionsvertrag zwischen CDU, CSU und SPD

21. Legislaturperiode

EU Privacy & Security Law



2.2. Bürokratierückbau, Staatsmodernisierung und moderne Justiz



Datenschutz entbürokratisieren

Wir reformieren die Datenschutzaufsicht und bündeln sie beim Bundesdatenschutzbeauftragten. Wir wollen unter Berücksichtigung des Grundrechts auf informationelle Selbstbestimmung und im Rahmen des europäischen Rechts Lösungen entwickeln, um im Datenschutzrecht aufwändige Einwilligungslösungen für eine komfortablere Nutzung staatlicher Serviceleistungen durch unbürokratische Widerspruchslösungen zu ersetzen.

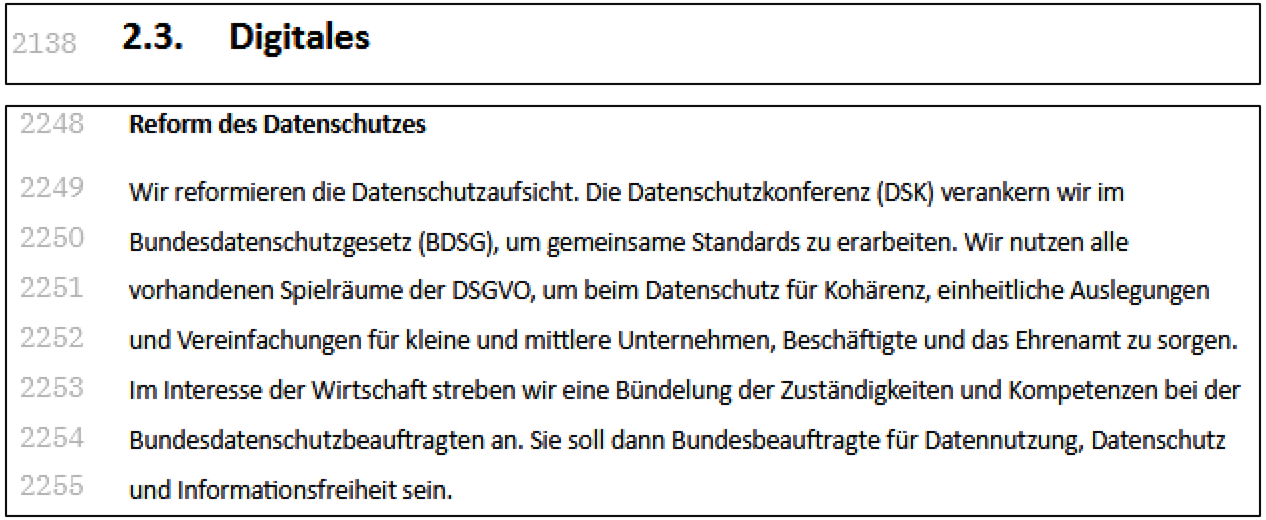
Die Datenschutzkonferenz (DSK) verankern wir im Bundesdatenschutzgesetz (BDSG), um gemeinsame Standards zu erarbeiten. Wir nutzen alle vorhandenen Spielräume der DSGVO, um beim Datenschutz für Kohärenz, einheitliche Auslegungen und Vereinfachungen für kleine und mittlere Unternehmen, Beschäftigte und das Ehrenamt zu sorgen. Auf europäischer Ebene wollen wir erreichen, dass nicht-kommerzielle Tätigkeiten (zum Beispiel in Vereinen), kleine und mittelständische Unternehmen und risikoarme Datenverarbeitungen (zum Beispiel Kundenlisten von Handwerkern) vom Anwendungsbereich der Datenschutzgrundverordnung ausgenommen werden. Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an. Sie soll dann Bundesbeauftragte für Datennutzung, Datenschutz und Informationsfreiheit sein.

Goal: Reduction of bureaucracy

Plan:

- Consent solutions are to be replaced by **objection solutions**
- Non-commercial activities, SMEs and low-risk data processing should be **excluded from the scope** of the GDPR

EU Privacy & Security Law



2.3. Digitales

Reform des Datenschutzes

Wir reformieren die Datenschutzaufsicht. Die Datenschutzkonferenz (DSK) verankern wir im Bundesdatenschutzgesetz (BDSG), um gemeinsame Standards zu erarbeiten. Wir nutzen alle vorhandenen Spielräume der DSGVO, um beim Datenschutz für Kohärenz, einheitliche Auslegungen und Vereinfachungen für kleine und mittlere Unternehmen, Beschäftigte und das Ehrenamt zu sorgen. Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an. Sie soll dann Bundesbeauftragte für Datennutzung, Datenschutz und Informationsfreiheit sein.

<u>Goal</u>: Data protection reform

<u>Plan</u>: Rather vague

“Use all existing flexibilities of the GDPR to ensure **consistency, uniform interpretations and simplifications** in data protection”

Questions & Contacts

Niko Härting

Partner and Founder of HÄRTING Rechtsanwälte

E-mail: haerting@haerting.de
Phone: +49 30 283057452