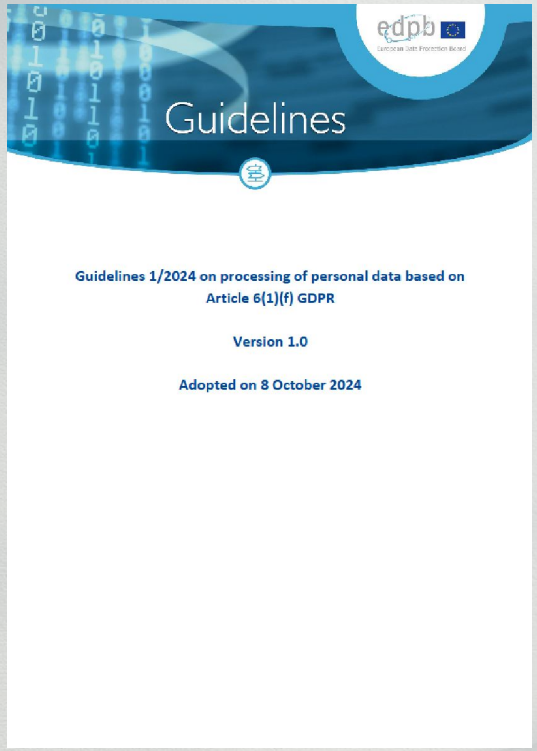
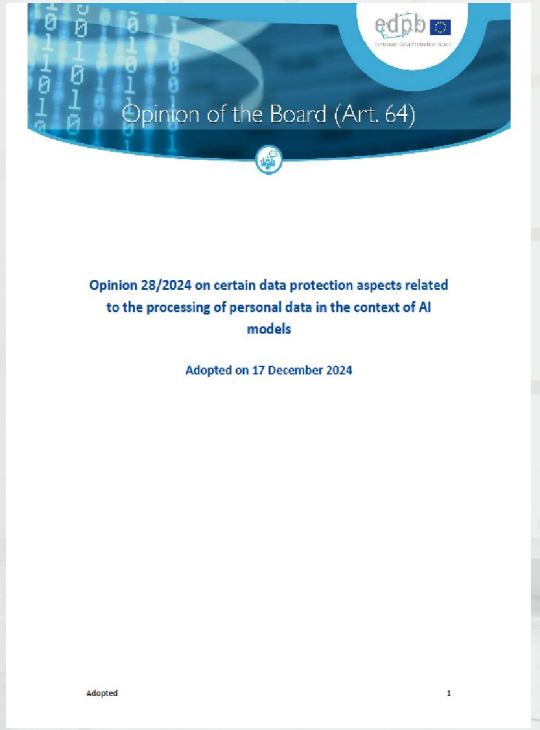
Ny veiledning fra EDPB om KI og berettiget interesse

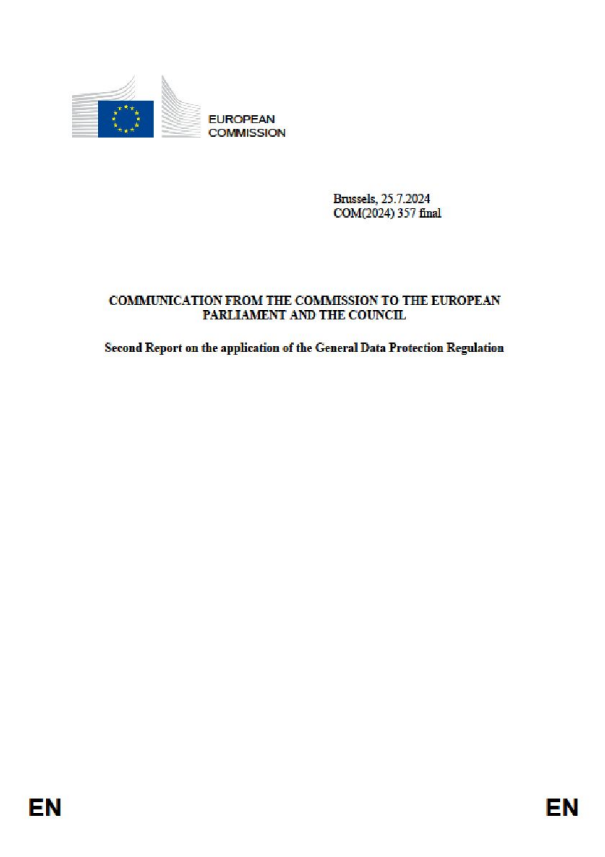




Luca Tosoni, PhD
Managing Associate, Schjødt
luca.tosoni@schjodt.com

Retningslinjer om berettiget interesse: kontekst og vedtakelsesprosess

- En prioritet for EU-kommisjonen og andre aktører



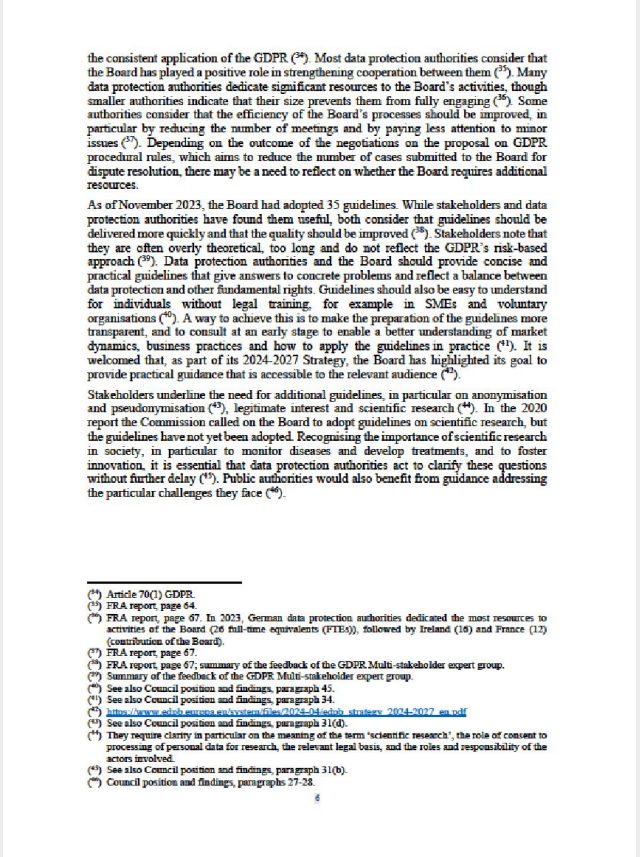
EUROPEAN COMMISSION

Brussels, 25.7.2024
COM(2024) 357 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Second Report on the application of the General Data Protection Regulation

EN EN

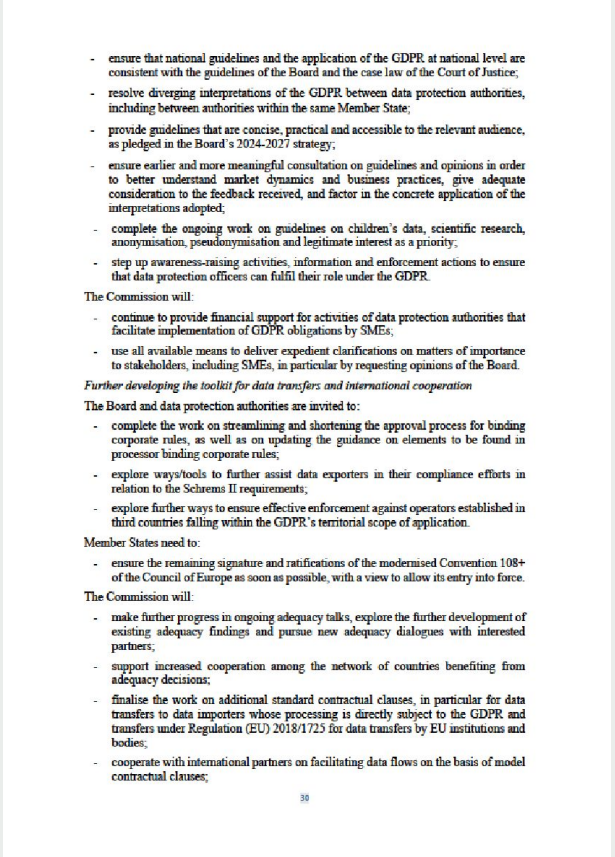


the consistent application of the GDPR ([34]). Most data protection authorities consider that the Board has played a positive role in strengthening cooperation between them ([35]). Many data protection authorities dedicate significant resources to the Board's activities, though smaller authorities indicate that their size prevents them from fully engaging ([36]). Some authorities consider that the efficiency of the Board's processes should be improved, in particular by reducing the number of meetings and by paying less attention to minor issues ([37]). Depending on the outcome of the negotiations on the proposal on GDPR procedural rules, which aims to reduce the number of cases submitted to the Board for dispute resolution, there may be a need to reflect on whether the Board requires additional resources.

As of November 2023, the Board had adopted 35 guidelines. While stakeholders and data protection authorities have found them useful, both consider that guidelines should be delivered more quickly and that the quality should be improved ([38]). Stakeholders note that they are often overly theoretical, too long and do not reflect the GDPR's risk-based approach ([39]). Data protection authorities and the Board should provide concise and practical guidelines that give answers to concrete problems and reflect a balance between data protection and other fundamental rights. Guidelines should also be easy to understand for individuals without legal training, for example in SMEs and voluntary organisations ([40]). A way to achieve this is to make the preparation of the guidelines more transparent, and to consult at an early stage to enable a better understanding of market dynamics, business practices and how to apply the guidelines in practice ([41]). It is welcomed that, as part of its 2024-2027 Strategy, the Board has highlighted its goal to provide practical guidance that is accessible to the relevant audience ([42]).

Stakeholders underline the need for additional guidelines, in particular on anonymisation and pseudonymisation ([43]), legitimate interest and scientific research ([44]). In the 2020 report the Commission called on the Board to adopt guidelines on scientific research, but the guidelines have not yet been adopted. Recognising the importance of scientific research in society, in particular to monitor diseases and develop treatments, and to foster innovation, it is essential that data protection authorities act to clarify these questions without further delay ([45]). Public authorities would also benefit from guidance addressing the particular challenges they face ([46]).

([34]) Article 70(1) GDPR.
([35]) FRA report, page 64.
([36]) FRA report, page 67. In 2023, German data protection authorities dedicated the most resources to activities of the Board (26 full-time equivalents (FTEs)), followed by Ireland (18) and France (12) (contribution of the Board).
([37]) FRA report, page 67.
([38]) FRA report, page 67; summary of the feedback of the GDPR Multi-stakeholder expert group.
([39]) Summary of the feedback of the GDPR Multi-stakeholder expert group.
([40]) See also Council position and findings, paragraph 45.
([41]) See also Council position and findings, paragraph 34.
([42]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf
([43]) See also Council position and findings, paragraph 31(d).
([44]) They require clarity in particular on the meaning of the term 'scientific research', the role of consent to processing of personal data for research, the relevant legal basis, and the roles and responsibility of the actors involved.
([45]) See also Council position and findings, paragraph 31(b).
([46]) Council position and findings, paragraphs 27-28.



- ensure that national guidelines and the application of the GDPR at national level are consistent with the guidelines of the Board and the case law of the Court of Justice;
- resolve diverging interpretations of the GDPR between data protection authorities, including between authorities within the same Member State;
- provide guidelines that are concise, practical and accessible to the relevant audience, as pledged in the Board's 2024-2027 strategy;
- ensure earlier and more meaningful consultation on guidelines and opinions in order to better understand market dynamics and business practices, give adequate consideration to the feedback received, and factor in the concrete application of the interpretations adopted;
- complete the ongoing work on guidelines on children's data, scientific research, anonymisation, pseudonymisation and legitimate interest as a priority;
- step up awareness-raising activities, information and enforcement actions to ensure that data protection officers can fulfil their role under the GDPR.

The Commission will:

- continue to provide financial support for activities of data protection authorities that facilitate implementation of GDPR obligations by SMEs;
- use all available means to deliver expedient clarifications on matters of importance to stakeholders, including SMEs, in particular by requesting opinions of the Board.

Further developing the toolkit for data transfers and international cooperation

The Board and data protection authorities are invited to:

- complete the work on streamlining and shortening the approval process for binding corporate rules, as well as on updating the guidance on elements to be found in processor binding corporate rules;
- explore ways/tools to further assist data exporters in their compliance efforts in relation to the Schrems II requirements;
- explore further ways to ensure effective enforcement against operators established in third countries falling within the GDPR's territorial scope of application.

Member States need to:

- ensure the remaining signature and ratifications of the modernised Convention 108+ of the Council of Europe as soon as possible, with a view to allow its entry into force.

The Commission will:

- make further progress in ongoing adequacy talks, explore the further development of existing adequacy findings and pursue new adequacy dialogues with interested partners;
- support increased cooperation among the network of countries benefiting from adequacy decisions;
- finalise the work on additional standard contractual clauses, in particular for data transfers to data importers whose processing is directly subject to the GDPR and transfers under Regulation (EU) 2018/1725 for data transfers by EU institutions and bodies;
- cooperate with international partners on facilitating data flows on the basis of model contractual clauses;

edpb
European Data Protection Board

Enforcement

Taskforce Fining

Cooperation

IT Users

Strategic Advisory

Key Provisions

Technology

International Transfers

BTLE

Coordinated Supervision Committee

External relations

Compliance, e-Government and Health

Financial Matters

Social Media

edpb
European Data Protection Board

Enforcement

Taskforce Fining

Cooperation

IT Users

Strategic Advisory

Key Provisions

Technology

International Transfers

BTLE

Coordinated Supervision Committee

External relations

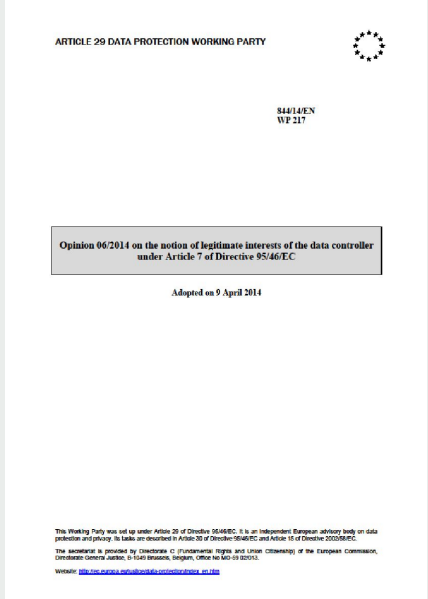
Compliance, e-Government and Health

Financial Matters

Social Media

Retningslinjer om berettiget interesse

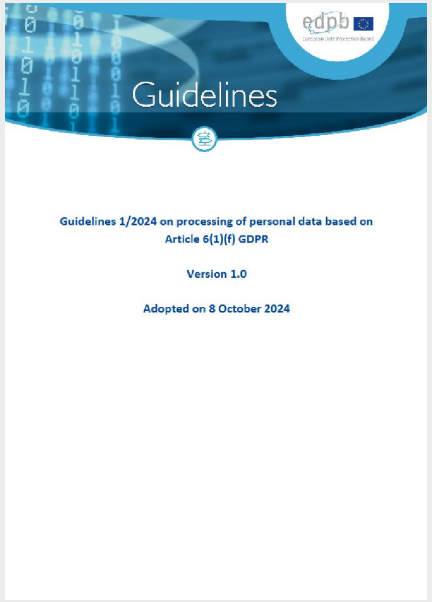
- Oppdater og bygger på WP29 Opinion 06/2014
- Vedtatt den 8. oktober 2024
- På høring frem til 20. november 2024
- Grunnlag for EDPB Opinion 28/2024 om AI-modeller


ARTICLE 29 DATA PROTECTION WORKING PARTY

844/14/EN
WP 217

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

Adopted on 9 April 2014



Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR

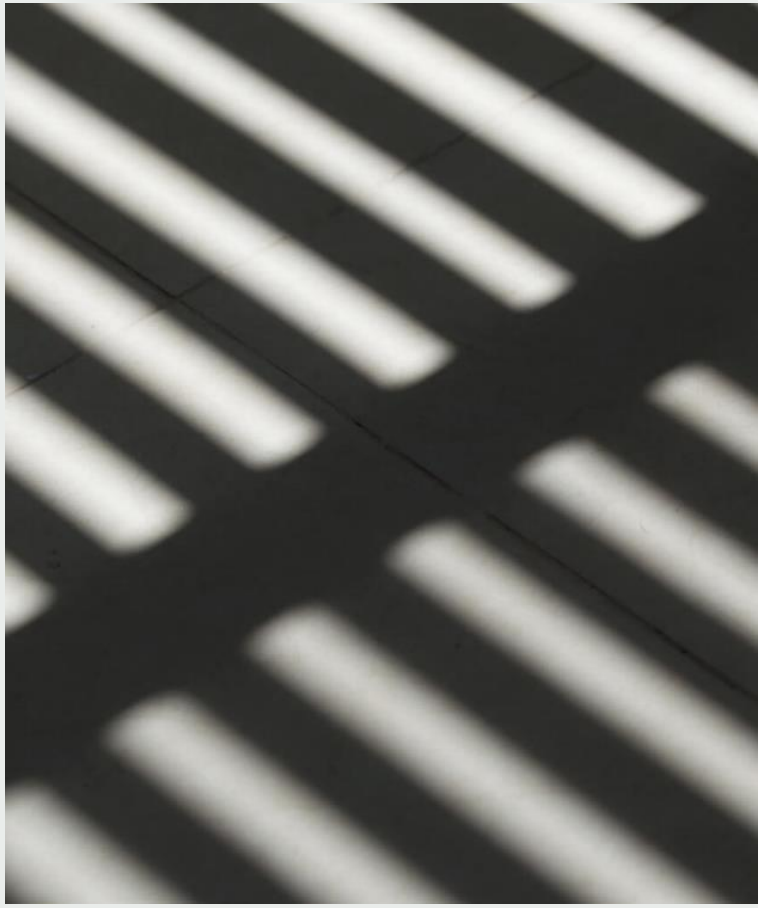
Version 1.0

Adopted on 8 October 2024

Retningslinjer om berettiget interesse

Vurdering av tre krav (som før):

- Berettiget interesse
- Nodvendighetskravet
- Balansetesten



Retningslinjer om berettiget interesse Hovednyheter

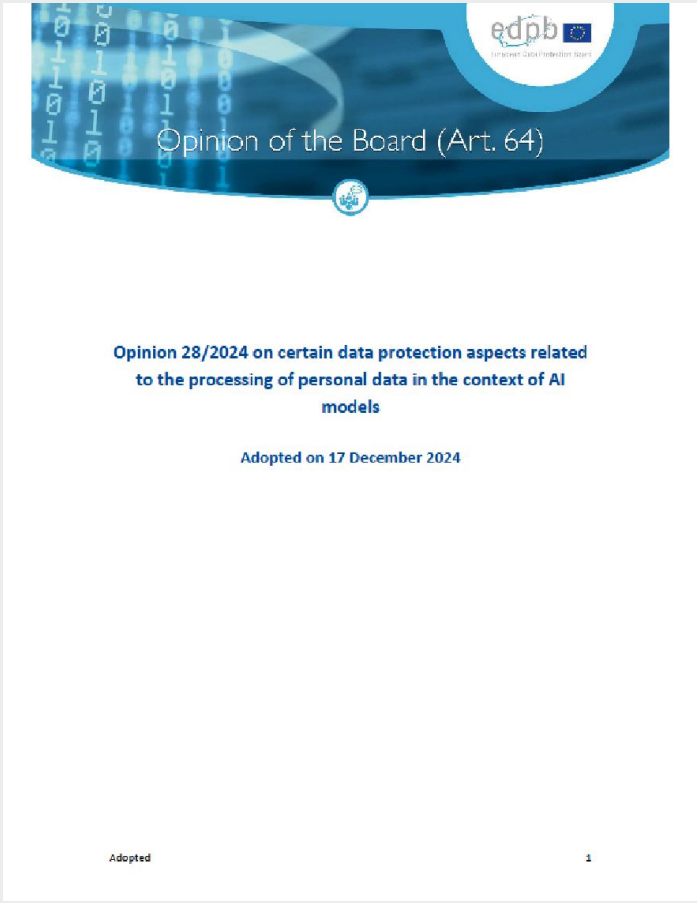
- En kommersiell interesse kan være en berettiget interesse (Sak C-621/22, *KNLTB*)
- Allmenne interesser ≠ interesser til tredjeparter
- Strengere dokumentasjonskrav
- Strengere transparenskrav
- Strengere nodvendighetskrav
- Høyere forventninger med hensyn til balansetesten
- Mange nye eksempler (f.eks. bedrageriforebygging, direkte markedsføring, osv.)
    - Ingen eksempler ang. KI

Opinion 28/2024 om AI-modeller

- Svar på spørsmål fra Datatilsynet i Irland
  - Begrepet «personopplysninger» og AI-modeller
  - Berettiget interesse som behandlingsgrunnlag for utvikling og bruk av KI

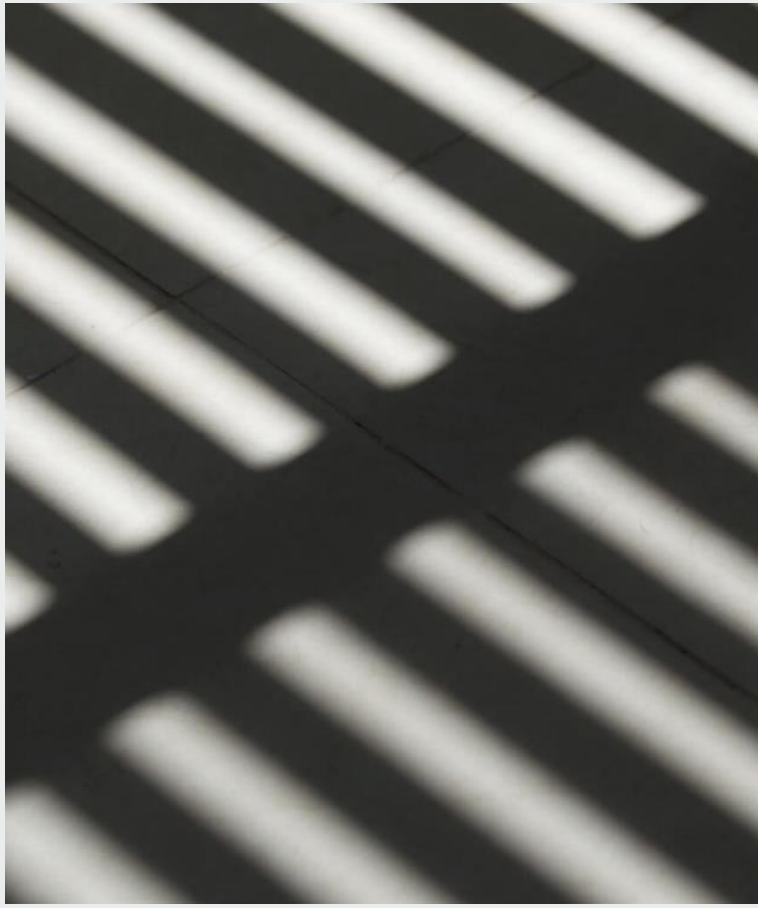
- Bygger delvis på retningslinjer om berettiget interesse
- Vedtatt den 17. desember 2024
- Hjemmel: GDPR artikkel 64 nr. 2 GDPR = kvasi-bindende
  - Kort frist for å vedta uttalelsen (8 + 6 uker)
  - Ingen høring

- Skal brukes av tilsynsmyndigheter i håndhevingshandlinger.
  - Allerede brukt av Datatilsynet i Italia i sin nylige avgjørelse mot OpenAI

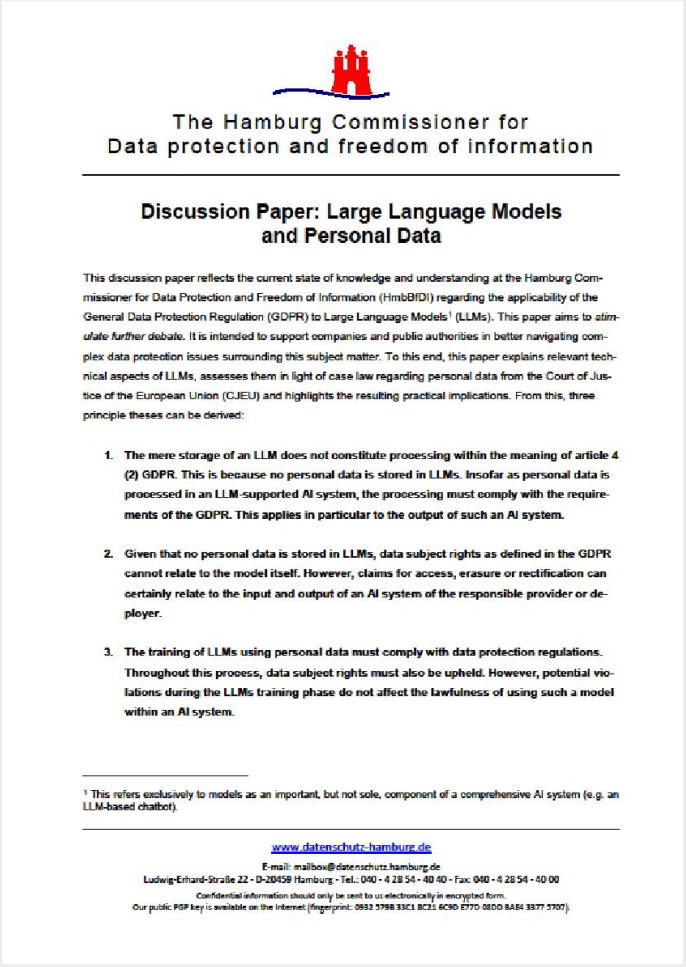


Når og hvordan en AI-modell kan anses som «anonym»?

- Skal vurderes fra sak til sak
- Man kan ikke legge til grunn at en AI-modell er «anonym»
- For at en AI-modell skal anses som anonym, må man vise at sannsynligheten for følgende er «ubetydelig» (insignificant):
  - direkte utvinning av personopplysninger om personer hvis personopplysninger ble brukt til å utvikle modellen
  - å få, med vilje eller ikke, slike personopplysninger gjennom forespørsler
- Skal dokumenteres av den behandlingsansvarlige
- Uttalelsen gir noen eksempler på metoder som kan brukes for å dokumentere dette



- Datatilsynet i Hamburg tolket dette annerledes



The Hamburg Commissioner for
Data protection and freedom of information

Discussion Paper: Large Language Models and Personal Data

This discussion paper reflects the current state of knowledge and understanding at the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) regarding the applicability of the General Data Protection Regulation (GDPR) to Large Language Models[1] (LLMs). This paper aims to *stimulate further debate*. It is intended to support companies and public authorities in better navigating complex data protection issues surrounding this subject matter. To this end, this paper explains relevant technical aspects of LLMs, assesses them in light of case law regarding personal data from the Court of Justice of the European Union (CJEU) and highlights the resulting practical implications. From this, three principle theses can be derived:

1. **The mere storage of an LLM does not constitute processing within the meaning of article 4 (2) GDPR. This is because no personal data is stored in LLMs. Insofar as personal data is processed in an LLM-supported AI system, the processing must comply with the requirements of the GDPR. This applies in particular to the output of such an AI system.**

2. **Given that no personal data is stored in LLMs, data subject rights as defined in the GDPR cannot relate to the model itself. However, claims for access, erasure or rectification can certainly relate to the input and output of an AI system of the responsible provider or deployer.**

3. **The training of LLMs using personal data must comply with data protection regulations. Throughout this process, data subject rights must also be upheld. However, potential violations during the LLMs training phase do not affect the lawfulness of using such a model within an AI system.**

[1] This refers exclusively to models as an important, but not sole, component of a comprehensive AI system (e.g. an LLM-based chatbot).

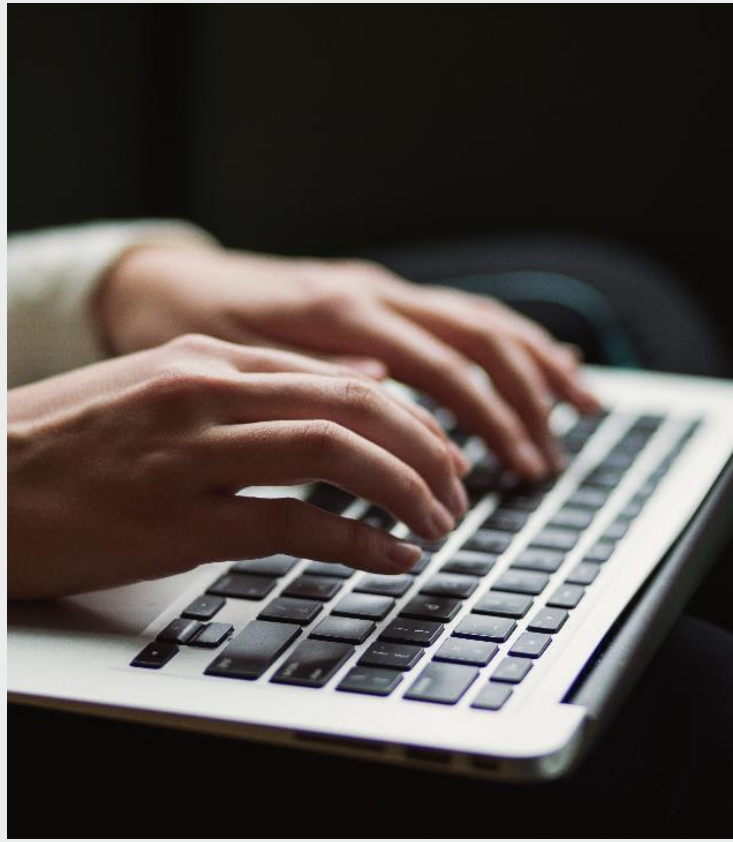
www.datenschutz-hamburg.de
E-mail: mailbox@datenschutz.hamburg.de
Ludwig-Erhard-Straße 22 - D-20459 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 - 40 00
Confidential information should only be sent to us electronically in encrypted form.
Our public PGP key is available on the Internet (fingerprint: 0932 5798 33C1 BC2E 6C90 E770 08DD 8AB4 3377 5707).

Berettiget interesse som behandlingsgrunnlag for utvikling og bruk av AI

I utgangspunktet er berettiget interesse et gyldig behandlingsgrunnlag

Vurdering av tre krav med hensyn til planlagt utvikling/bruk av AI:

- Berettiget interesse
- Nodvendighetskravet
- Balansetesten



Berettiget interesse som forfølges av den behandlingsansvarlige eller en tredjepart

- Den berettigede interessen må være lovlig, klart definert på forhånd, reell og saklig begrunnet i virksomheten.

- Eksemplene i Opinion 28/2024: «the following examples may constitute a legitimate interest in the context of AI models: (i) developing the service of a conversational agent to assist users; (ii) developing an AI system to detect fraudulent content or behaviour; and (iii) improving threat detection in an information system.»

Nodvendighetskrav

- Den aktuelle behandlingen av personopplysninger må være nødvendig for denne interessen.
- Det vil si at virksomheten må vurdere om den kan oppnå formålet på en måte som bedre varetar personvernet.
- Man må altså velge den behandlingen som er minst inngripende. Kan målet nås gjennom en mindre inngripende behandling?
- Mengden data som skal behandles er en viktig faktor (data minimering).
- Eksempel: «For example, and as the case may be, the intended volume of personal data involved in the AI model needs to be assessed in light of less intrusive alternatives that may reasonably be available to achieve just as effectively the purpose of the legitimate interest pursued».

Balansetesten

- Virksomheten må foreta en interesseavveining for å avgjøre om den enkeltes interesser og rettigheter veier tyngre enn virksomhetens berettigede interesse
    - Eksempler: “In the context of the development phase of an AI model, these may include, but are not limited to, the interest in self-determination and retaining control over one’s own personal data (e.g. the data gathered for the development of the model). In the context of the deployment of an AI model, the data subjects’ interests may include, but are not limited to, interests in retaining control over one’s own personal data (e.g. the data processed once the model is deployed), financial interests (e.g. where an AI model is used by the data subject to generate revenues, or is used by an individual in the context of their professional activity), personal benefits (e.g. where an AI model is used to improve accessibility to certain services), or socioeconomic interests (e.g. where an AI model enables access to better healthcare, or facilitates the exercise of a fundamental right such as access to education)”.
- Berettiget forventninger
    - Berettiget forventninger ≠ praksis i bransjen
    - De er ikke nødvendigvis avhengige av innholdet i personvernavklaring
    - Gjennomsnittlig individ
- Tiltak for å minimere personvernkonsekvensene
    - Eksempler: «Release of public and easily accessible communications which go beyond the information required under Article 13 or 14 GDPR, for instance by providing additional details about the collection criteria and all datasets used, taking into account special protection for children and vulnerable persons. Alternative forms of informing data subjects, for instance: media campaigns with different media outlets to inform data subjects, information campaign by e-mail, use of graphic visualisation, frequently asked questions, transparency labels and model cards the systematisation of which could structure the presentation of information on AI models, and annual transparency reports on a voluntary basis.»

OpenAI sak i Italia

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

COMUNICATO STAMPA - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro.

- English version

VEDI ANCHE

- Provvedimento del 2 novembre 2024
- Comunicato del 28 aprile 2023
- Comunicato del 13 aprile 2023
- Comunicato del 12 aprile 2023
- Provvedimento dell'11 aprile 2023
- Comunicato dell'8 aprile 2023
- Comunicato del 6 aprile 2023
- Comunicato del 4 aprile 2023
- Comunicato del 31 marzo 2023
- Provvedimento del 30 marzo 2023

ChatGPT, il Garante privacy chiude l'istruttoria
OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro.

Il Garante per la protezione dei dati personali ha adottato nei giorni scorsi un provvedimento correttivo e sanzionatorio nei confronti di OpenAI in relazione alla gestione del servizio ChatGPT.

Il provvedimento, che accerta le violazioni a suo tempo contestate alla società californiana, arriva all'esito di un'istruttoria avviata nel marzo del 2023 e dopo che l'EDPB (Comitato europeo per la protezione dei dati) ha pubblicato il parere con il quale identifica un approccio comune ad alcune delle più rilevanti questioni relative al trattamento dei dati personali nel contesto della progettazione, sviluppo e distribuzione di servizi basati sull'intelligenza artificiale.

Secondo il Garante la società statunitense, che ha creato e gestisce il chatbot di intelligenza artificiale generativa, oltre a non aver notificato all'Autorità la violazione dei dati subita nel marzo 2023, ha trattato i dati personali degli utenti per addestrare ChatGPT senza aver prima individuato un'adeguata base giuridica e ha violato il principio di trasparenza e i relativi obblighi informativi nei confronti degli utenti. Per di più, OpenAI non ha previsto meccanismi per la verifica dell'età, con il conseguente rischio di esporre i minori di 13 anni a risposte inidonee rispetto al loro grado di sviluppo e autoconsapevolezza.

L'Autorità, con l'obiettivo di garantire, innanzitutto, un'effettiva trasparenza del trattamento dei dati personali, ha ordinato a OpenAI, utilizzando per la prima volta i nuovi poteri previsti dall'articolo 166, comma 7 del Codice Privacy, di realizzare una campagna di comunicazione istituzionale di 6 mesi su radio, televisione, giornali e Internet.

I contenuti, da concordare con l'Autorità, dovranno promuovere la comprensione e la consapevolezza del pubblico sul funzionamento di ChatGPT, in particolare sulla raccolta dei dati di utenti e non-utenti per l'addestramento dell'intelligenza artificiale generativa e i diritti esercitabili dagli interessati, inclusi quelli di opposizione, rettifica e cancellazione.

Grazie a tale campagna di comunicazione, gli utenti e i non-utenti di ChatGPT dovranno essere sensibilizzati su come opporsi all'addestramento dell'intelligenza artificiale generativa con i propri dati personali e, quindi, essere effettivamente posti nelle condizioni di esercitare i propri diritti ai sensi del GDPR.

Il Garante ha comminato a OpenAI una sanzione di quindici milioni di euro calcolata anche tenendo conto dell'atteggiamento collaborativo della società.

Infine, tenuto conto che la società, nel corso dell'istruttoria, ha stabilito in Irlanda il proprio quartier generale europeo, il Garante, in ottemperanza alla regola del c.d. one stop shop, ha trasmesso gli atti del procedimento all'Autorità di protezione dati irlandese (DPC), divenuta autorità di controllo capofila ai sensi del GDPR, affinché prosegua l'istruttoria in relazione a eventuali violazioni di natura continuativa non esauritesi prima dell'apertura dello stabilimento europeo.

Roma, 20 dicembre 2024

ChatGPT, The Italian Data Protection Authority closes the preliminary investigation
OpenAI will have to carry out a six-month information campaign and pay a fine of EUR 15 million

The Italian Data Protection Authority has recently taken corrective and sanctioning measures against OpenAI in relation to the management of the ChatGPT service.

The measure, which ascertains the breaches that were contested with the Californian company at the time, reaches the result of an investigation initiated in March 2023 and after the EDPB (European Data Protection Board) published its opinion identifying a common approach to some of the most important issues related to the processing of personal data in the context of the design, development and deployment of AI-based services.

According to the Italian Data Protection Authority, the US company, which created and manages the generative artificial intelligence chatbot, did not notify the Authority of the data breach it underwent in March 2023, it has processed users' personal data to train ChatGPT without first identifying an appropriate legal basis and has violated the principle of transparency and the related information obligations toward users. Furthermore, OpenAI has not provided for mechanisms for age verification, which could lead to the risk of exposing children under 13 to inappropriate responses with respect to their degree of development and self-awareness.

The Authority, with the aim of ensuring, first and foremost, effective transparency in the processing of personal data, ordered OpenAI - using for the first time the new powers provided for in article 166 paragraph 7 of the Privacy Code - to carry out a 6-month institutional communication campaign on radio, television, newspapers and the Internet.

The content, to be agreed with the Authority, should promote public understanding and awareness of the functioning of ChatGPT, in particular on the collection of user and non-user data for the training of generative artificial intelligence and the rights exercised by data subjects, including the rights to object, rectify and delete their data.

Through this communication campaign, users and non-users of ChatGPT will have to be made aware of how to oppose generative artificial intelligence being trained with their personal data and thus be effectively enabled to exercise their rights under the GDPR.

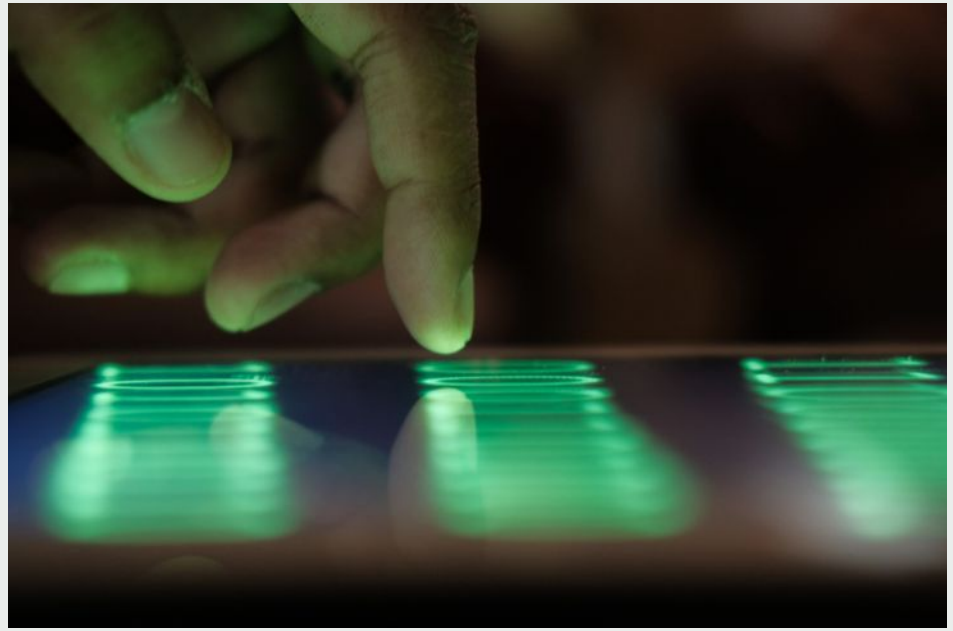
The Data Protection Authority imposed a fine of EUR 15 million on OpenAI, which was also calculated taking into account the company's cooperative attitude.

Finally, in view of the fact that the company established its European headquarters in Ireland in the course of the preliminary investigation, the Data Protection Authority, in compliance with the so-called one stop shop mechanism, forwarded the procedural documents to the Irish Data Protection Authority (DPC), which became lead supervisory authority under the GDPR so as to continue investigating any ongoing infringements that have not been exhausted before the opening of the European headquarters.

Rome, 20 December 2024

Kommende retningslinjer som er relevant for KI

- Guidelines on Data Scraping
- Guidelines on the Interplay Between the AI Act and the GDPR
- Guidelines on Anonymization



Rettskildemessig verdi av EDPB-retningslinjer

- Grimaldi (C-322/88):

  «the measures in question cannot therefore be regarded as having no legal effect. The national courts are bound to take recommendations into consideration in order to decide disputes submitted to them, in particular where they cast light on the interpretation of national measures adopted in order to implement them or where they are designed to supplement
  Binding Community provisions».

- FBF c. ACPR (C-911/19):

  «It is also for the national courts to take into consideration EBA Guidelines in order to resolve the disputes submitted to them, in particular when those guidelines are, like the contested guidelines, intended to supplement binding provisions of European Union law».

Dansk Rørindustri (C-189/02 P, C-202/02 P, da C-205/02 P a C-208/02 P e C-213/02 P):

«In adopting such rules of conduct and announcing by publishing them that they will henceforth apply to the cases to which they relate, the institution in question imposes a limit on the exercise of its discretion and cannot depart from those rules under pain of being found, where appropriate, to be in breach of the general principles of law, such as equal treatment or the protection of legitimate expectations. It cannot therefore be precluded that, on certain conditions and depending on their content, such rules of conduct, which are of general application, may produce legal effects».

Schjødt

Tusen takk!

Noen spørsmål?

Luca Tosoni, PhD
Managing Associate
m: +47 40 18 55 98
d: +47 23 01 19 85
luca.tosoni@schjodt.com