Legal Opinion

Inadmissibility of Meta's processing of social media data for AI training

LAW FIRMI:	Simpliant Legal PartG mbB
AUTHOR:	Steffen Gross (Attorney-at-law, Berlin, Germany)
DATE:	May 19, 2025
VERSION:	1.0 (English)
NOTICE OF USE:	This opinion is intended for public and free distribution.

Simpliant

Table of contents

1 Executive Summary

This legal opinion examines the admissibility under data protection law of Meta Platforms Ireland Ltd. ("Meta")'s planned processing of personal data of users in the European Union for the training of generative AI models (in particular LLaMA).

The legal assessment concludes that the planned processing is incompatible with the provisions of the General Data Protection Regulation (GDPR) in several essential respects and is therefore unlawful.

1. Unlawful processing of special categories of personal data (Art. 9 GDPR)

The data processing inevitably also includes information that allows conclusions to be drawn about political opinions, health status, religious beliefs, or sexual orientation. There is no valid exception under Art. 9 (2) GDPR for these particularly sensitive types of data. In particular, there is no explicit consent from the data subjects.

2. Lack of legal basis under Art. 6(1)(f) GDPR (legitimate interest)

Meta cannot effectively rely on a legitimate interest either. The necessity of comprehensive data processing has not been demonstrated.

The balancing of interests also weighs against Meta. The decisive factors are the nature and sensitivity of the data processed, the depth and lack of transparency of the processing in the context of AI training, the structural loss of control of the data subjects, insufficient objection mechanisms, and the risk of irreversible further use as a result of the planned open-source publication.

3. Further violations of key GDPR requirements

Transparency (Art. 12–14 GDPR): The information provided on data processing is insufficient, incomplete, and does not meet the transparency requirements under data protection law.

Rights of data subjects (Art. 15–21 GDPR): Effective exercise of the rights to information, objection, and erasure is not guaranteed in practice.

Data protection impact assessment (Art. 35 GDPR): Due to the systemic risk, a DPIA would have been mandatory. There is no evidence of a DPIA having been carried out or of any subsequent consultation with the competent supervisory authority (Art. 36 GDPR).

4. Legal and economic consequences

The identified violations of the GDPR pose significant regulatory and civil law risks for Meta.

Regulatory measures pursuant to Art. 58 and 83 GDPR are possible, including prohibitions on processing, orders to delete data, and fines of up to 4% of global annual revenue—potentially amounting to billions.

Under civil law, Article 82 GDPR gives rise to claims for non-material damages; even a loss of control over personal data may be sufficient for this. Damages in the four-digit range per person are realistic and, if widely asserted, would lead to significant financial risks.

5. Conclusion

Meta's planned data processing for training generative AI models with user data from the Facebook and Instagram platforms violates key provisions of the GDPR in several respects.

The processing is therefore unlawful and is likely to entail significant regulatory and civil law risks for Meta.

2 Facts and subject matter of the opinion

Facts

Meta Platforms Ireland Ltd. ("Meta") intends to train generative AI models – including large open-source language models such as "LLaMA" – using data from users in the European Union.

The Facebook and Instagram platforms, operated by Meta Platforms Inc. and Meta Platforms Ireland Ltd., collect and process a wide range of personal data. Depending on usage behavior and profile settings, the following data in particular is collected:

- Activity and content data: posts, comments, likes, reactions, uploaded photos and videos, stories, reels, live content, and metadata from direct messages.
- Profile data: biographies, profile pictures, interests, relationship status, and other information provided by users,
- Technical and device-related data: device type, operating system, app version, IP address, location data, device identifiers, cookies, advertising IDs, and usage time,
- Usage behavior and social connections: content viewed, scrolling and clicking behavior, interactions with advertising, story views and profile visits, friend and follower structures, communication histories, interactions with other users,
- External data sources: activities on third-party sites with Facebook/Instagram integration, uploaded contact lists, and data from advertising partners and analytics providers
- Derived profile information: interest profiles, preferences, presumed political, religious, or commercial attitudes, consumer behavior, and target group assignments.

Data collection and processing takes place across platforms. In the case of linked user accounts or shared device use, information from both platforms is merged and analyzed together. In addition, Meta also processes interactions with AI systems, in particular questions asked. The aim of AI training is to adapt generative AI to the linguistic, cultural, and social characteristics of European users.

Meta states that no private messages and no content from persons under the age of 18 will be included in the training. Users in the EU have been informed about the intended data processing. An objection form is provided that can be used to refuse the use of public content for training purposes.

In terms of data protection law, Meta cites a legitimate interest within the meaning of Art. 6 (1) f) GDPR as the legal basis and takes the view that the planned processing is in line with the requirements of the GDPR.

Subject matter of the opinion

The following legal opinion focuses on the question of whether the planned data processing can be based on an effective legal basis and is compatible with the provisions of the General

Data Protection Regulation, in particular taking into account Art. 6(1)(f) and Art. 9 GDPR. If this is not the case, the resulting legal consequences shall be outlined in summary form.

3 Legal assessment

3.1 Applicability of the GDPR

The provisions of the General Data Protection Regulation ("GDPR") apply to the present case. The material scope of application pursuant to Art. 2 GDPR is established, as automated personal data is processed that is attributable to identifiable persons in the EU. The territorial scope pursuant to Art. 3 (1) and (2) (a) GDPR is also given, as Meta is based in the EU and specifically offers its services to persons in the EU.

3.2 Special categories of personal data (Art. 6, 9 (2) GDPR)

The planned use of personal content from Facebook and Instagram profiles for training generative AI models requires a sound legal basis, Art. 6 GDPR.

First, it must be examined whether special categories of personal data within the meaning of Art. 9 para. 1 GDPR are affected. If this is the case, processing is generally prohibited unless one of the exceptions in Art. 9 para. 2 GDPR applies.

Processing of special categories of personal data (Art. 9 GDPR)

Special categories of personal data pursuant to Art. 9 GDPR include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and [...] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Art. 9 (1) GDPR applies regardless of whether the information disclosed through processing is accurate or whether the controller intends to process data of a special category. The only decisive factor is whether the processed data objectively allows conclusions to be drawn about particularly sensitive information within the meaning of Art. 9 (1) GDPR.[1]

The content to be evaluated on Facebook and Instagram includes, among other things, texts, images, comments, reactions, "likes," group memberships, and other interactions of users.

Due to the scope, social function, and typical use of these platforms, a significant portion of the processed content allows direct or indirect conclusions to be drawn about special categories of personal data within the meaning of Art. 9(1) GDPR.

Specifically, it can be assumed that the content:

- political opinions are recognizable, for example through shared posts, political statements, group memberships, or reactions to political content;
- religious or ideological beliefs are expressed, e.g., in the form of profile information, references to holidays, quotations, or symbolic representations;
- health data is disclosed, for example through reports on illnesses, treatments, mental states, or calls for support;

[1] CJEU Judgment of 4 July 2023, C-252/21, para. 69.

- sexual orientation or aspects of sexual life are addressed or visualized, for example in relationship details, couple photos, comments, or through the representation of sexual identities.

In addition, the content on the platforms, such as images with contextual information, group memberships, and "likes," often allows the combination of several individual characteristics to facilitate conclusions to be drawn about the above-mentioned data categories.

The planned processing by Meta therefore includes special categories of personal data within the meaning of Art. 9 para. 1 GDPR. Data processing is therefore only permissible if one of the exceptions listed exhaustively in Art. 9 (2) GDPR is fulfilled.

Examination of the exceptions (Art. 9 (2) GDPR)

Consent Art. 9 (2) a) GDPR

The data subjects have not given their explicit consent within the meaning of Art. 9 (2) (a) GDPR to the use of their (sensitive) data and content for the training of AI models. Merely providing information about the data processing by Meta and the possibility of objection (opt-out) does not satisfy the legal requirements for voluntary, informed, and explicit consent.

Data made manifestly public (Art. 9 para. 2 e) GDPR)

Nor is the data in question data made manifestly public within the meaning of (Art. 9 para. 2 e) GDPR).

Although content on Facebook and Instagram may be (partially) publicly visible, this does not mean that it has been "manifestly made public" within the meaning of the standard. The European Data Protection Board clarifies that a blanket assumption of public accessibility is not permissible. The context of the publication is decisive.

On social networks, communication is regularly directed at a limited target group. Visibility often results from default settings or platform mechanisms that are neither fully transparent nor known to users. There is no publication with the intention of making content available to the general public for unrestricted reuse, in particular for training generative AI.

In the absence of a relevant exception under Art. 9(2) GDPR, the processing of special categories of personal data is not permissible in the present case.

An appeal to Art. 6(1)(f) GDPR is ruled out, as this would otherwise undermine the specific legal requirements of Art. 9(2) GDPR.

The following examination is therefore only carried out as a precautionary measure and has no justifying effect with regard to the inadmissibility under Article 9 GDPR.

3.3 In the alternative: Legitimate interest (Article 6(1)(f) GDPR)

Data processing on the basis of Article 6(1)(f) GDPR is permissible if the following conditions are cumulatively met:

1. the user has been informed of the legitimate interest of the controller,

2. the processing is absolutely necessary to achieve this interest,
3. and a balancing of interests shows that the rights and freedoms of the users do not outweigh this interest.[2]

Stage 1: Existence of a legitimate interest

An interest within the meaning of Art. 6 para. 1 f) GDPR is the benefit that the controller intends to derive from the processing. It is considered legitimate if it is lawful, specific, clearly formulated, and current.[3]

Meta states that it trains generative AI models such as LLaMA with user data in order to adapt them to the linguistic, cultural, and social characteristics of European users. In addition, there is an economic interest in improving product quality and competitiveness. The development and optimization of generative AI systems can, in principle, represent legitimate economic, ideological, and technical interests.

However, doubts already exist as to whether the stated purpose is sufficiently clear and precise. Meta remains vague and does not specify which data is processed or for what specific purposes the processing is carried out. This raises the question of whether the requirements for transparency and precise purpose specification are met.

However, this question can be left open if the legitimate interest does not hold up in the further examination, for example due to a lack of necessity or the overriding interests of the data subjects.

Stage 2: Necessity of processing

The processing of personal data must be necessary to pursue the legitimate interest. The necessity is assessed in two stages in accordance with EDSA Opinion 28/2024 (para. 72): The processing must (1) be suitable for achieving the objective and (2) there must be no equally effective but less intrusive alternatives available. The burden of proof for necessity lies with the controller, i.e. Meta (Art. 5 (2) GDPR).

Suitability:

The processing of content from European users of Facebook and Instagram and their interactions with AI systems appears to be fundamentally suitable for adapting AI models to linguistic, cultural, and social characteristics.

No less intrusive means with the same effect:

Processing is not necessary if the intended purpose can be achieved by less intrusive means. The ECJ emphasizes that the principle of data minimization pursuant to Art. 5 (1) lit. c GDPR must be taken into account: Only data that is actually necessary for the specific purpose may

[2] CJEU Judgment of 4 July 2023, C-252/21, para. 69.

[3] EDPB 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, para. 68.

be processed.[4] If the purpose can also be achieved with less or non-personal data, the processing of personal data is not permitted.[5]

Meta states that it does not include private messages or content from minors. Although this reduces the intensity of the interference, it does not prove the necessity of the chosen method.

The decisive factor is whether the objective – the adaptation of AI models – could also be achieved by less intrusive means, in particular by using a smaller amount of data, anonymized or synthetic data.

Meta bears the burden of proving why alternatives such as synthetic data are unsuitable. A blanket assertion that personal data is more suitable is not sufficient. The planned comprehensive use of all Facebook and Instagram content without any discernible differentiation according to data type, visibility, or relevance is not necessary and therefore violates the principle of data minimization. A targeted, purpose-related selection would be necessary.

Interim conclusion:

The necessity of data processing to the extent intended by Meta has not been demonstrated in a comprehensible manner. There are considerable doubts as to whether the intended purpose could not also be achieved by less intrusive measures. Thus, the second requirement of Art. 6 (1) (f) GDPR is not fulfilled.

Stage 3: No overriding interests or fundamental rights of the data subjects

Even if a legitimate interest and the necessity of the processing were affirmed, the processing would only be permissible if the interests or fundamental rights and freedoms of the data subjects do not outweigh them (Art. 6 para. f) GDPR). The balancing test must be carried out taking into account all relevant circumstances.

When weighing up the interests, particular consideration must be given to the nature, sensitivity and quantity of the data processed, the scope and purpose of the processing, the intensity of the interference, the vulnerability of the data subjects (e.g., minors), the legitimate expectations of users, the transparency and traceability of the data processing, and the existence or absence of appropriate technical and organizational safeguards.

In the present case, the legitimate interests of the data subjects outweigh the interests of the data controller:

1. Type and sensitivity of the data

The content processed is personal data from social media profiles, in particular text posts, interactions, and a large number of images. This data is highly relevant to the individual and allows conclusions to be drawn about opinions, living conditions, social relationships, locations, and emotional states.

[4] CJEU Judgment of 4 October 2024 – C-446/21, para. 59.

[5] EDPB 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, para. 73.

It also includes special categories of personal data within the meaning of Article 9(1) GDPR, such as political opinions, religious beliefs, health information, or sexual orientation, even if these are not explicitly stated but only implied (see above).

2. Scope, duration, and extent of data processing

The planned data processing affects around 260 million user profiles per platform (Facebook and Instagram). The data covers long periods of time (usually several years) and documents the personal development of the data subjects in mostly high granularity.

In combination, the platforms thus have one of the most comprehensive personal data sets in the world, which can be used to reconstruct a precise digital personality profile of almost every data subject.

Furthermore, the processing is not limited to individual pieces of information, but is model-based and aggregated across a large number of data sources, to an extent, duration, and scope that is hardly ever transparent or controllable for the data subject.

Thanks to their comprehensive data infrastructure, cross-platform consolidation of information, and use of sophisticated analysis and profiling technologies, the platforms can create detailed personality profiles and draw far-reaching conclusions about users' behavior, attitudes, and living conditions.

3. Lack of transparency and loss of control through AI processing

The training of generative AI models is technically highly complex, incomprehensible to data subjects, and impossible to verify retrospectively. Once trained, models function as so-called "black boxes": they convert personal content into high-dimensional model parameters, making targeted assignment, deletion, or correction pursuant to Art. 15, 16, or 17 of the GDPR practically impossible. It is neither possible to reconstruct which specific data was used in training nor to trace the influence this data has on the model's subsequent output.

This contradicts the principle of transparency under Art. 5 (1) a) GDPR and significantly impairs the right to informational self-determination. Since data subjects have no insight into the content used and neither control nor effective deletion is possible, there is a lack of effective legal protection within the meaning of the GDPR.

4. Insufficient safeguarding of rights to object

Meta does provide an opt-out option, for example via an in-app objection form. However, there is no guarantee that the personal data of data subjects will actually be completely excluded from the training of generative AI models after an objection has been lodged.

- Indirect processing may still take place, for example:
- through photos in which objecting persons or children are also depicted,
- through comments, tags, or content created by third parties,
- through embedding in social networks or data clusters where connections to objecting persons exist.

Data from persons who have either exercised their right to object or who were unable to give informed consent (e.g., minors) may still be included in the training material in this way. This constitutes processing against the declared will of the data subject and contradicts the right to object enshrined in Art. 21 GDPR.

5. No expectation and impermissible change of purpose

The content provided by users on Facebook and Instagram was published in the context of social interaction – not with the aim of being analyzed by machines or used for training generative AI models. Social media platforms are not entirely public spaces, but semi-public communication environments whose content is often restricted by privacy settings. This distinguishes them significantly from openly accessible websites.

The planned use of this data for AI training constitutes a change of purpose within the meaning of Art. 6 (4) GDPR. Such a change is only permissible if it is compatible with the original purpose of the collection or if there is a new legal basis, in particular taking into account the criteria set out in Art. 6 (a) to (e) GDPR. Given the differences in content and technology between social communication and data-intensive model development, the necessary compatibility of purposes is lacking.

Furthermore, when creating their accounts, users could not have expected that their content would be used in the future to train highly complex AI systems.

6. Reproductions that violate personal rights

Previously documented incidents show that generative AI models – in particular large language models (LLMs) – tend to make false, misleading, or defamatory statements about real people.

Based on the training data, LLMs can hallucinate content, i.e., invent information that appears true but is factually incorrect. This can also include real names, biographical data, or sensitive information reproduced in an inappropriate context. These risks affect not only prominent individuals but also average users.

Affected individuals have no influence over the processing of their data or the representation of their person in the output of such a model. In particular, there are no or only very limited possibilities for rectification, deletion, or subsequent correction of inaccurate model representations.

7. Risk of re-identification and data extraction from LLMs

Research findings show that personal data that has been incorporated into the training of large language models can be extracted from the model again. Several studies have demonstrated that LLMs—especially when prompted specifically—can reproduce content such as real names, addresses, telephone numbers, or sensitive information (e.g., health data), even if this was not publicly accessible but originated from training data.

Even in models with billions of parameters, confidential training data can be recovered using systematic methods.[6] The possibility of re-identification contradicts the principle of data

[6] "Extracting Training Data from Large Language Models", available at https://arxiv.org/abs/2012.07805.

minimization pursuant to Art. 5 (1) c) GDPR and the obligation to ensure the confidentiality and integrity of personal data (Art. 5 (1) f), Art. 32 GDPR).

Since it cannot be ruled out that personal data can be extracted from the model or assigned to individual persons, there is no verifiably irreversible anonymization.

8. Risk of complete loss of control through open-source publication

As in the case of LLaMA 2, Meta plans to continue publishing trained generative AI models as open source in the future. This means that the model, including its parameters, will be made publicly available and can be downloaded, reused, fine-tuned, or used as the basis for new models ("derivative models") by third parties worldwide.

However, once models have been published, they can no longer be controlled: Neither Meta nor a supervisory authority can effectively track how and by whom the model is reused, or whether personal content contained therein is extracted or processed in subsequent applications. Furthermore, claims for correction, deletion, or information pursuant to Art. 15 et seq. GDPR cannot be enforced against downstream actors in practice—especially since they often operate outside the European legal area and cannot be identified.

The associated loss of control constitutes a particularly serious interference with the fundamental right to informational self-determination.

Interim conclusion:

In view of the particular sensitivity of the data concerned, the extreme depth and scope of the processing, the technical opacity, the risks to personal rights, and the irreversible loss of control, it must be concluded that the interests and fundamental rights of the data subjects clearly outweigh Meta's economic interest in optimizing generative AI models.

Processing pursuant to Art. 6 (1) (f) GDPR on the basis of legitimate interests is therefore not permissible in the present case.

3.4 Transparency and information obligations (Art. 12 - 14 GDPR)

Meta provides information on data processing in connection with "AI at Meta" in its "Privacy Center." It explains that generative AI models are based on "billions of pieces of information" sourced from "publicly available sources" and "our products and services." It also states that any user interactions with AI features may be used to improve the models. Users have the right to object to such use.

However, it remains unclear which specific categories of personal data are used for AI training. The purpose of the processing is also only described in general terms as "model improvement," without indicating a precise purpose within the meaning of Art. 5(1)(b) GDPR.

Furthermore, there is no clear description of how the model training is carried out, for example, whether and to what extent message content, posts, photos, videos, or other specific interactions are affected. Nor is it explained how deleted data is handled and to what extent such deletions affect models that have already been trained.

The information provided is abstract, general, and leaves essential questions regarding data processing unanswered, meaning that it does not meet the requirement for clear, transparent, and easily understandable information within the meaning of Art. 12, 13, and 14 of the GDPR.

The explanations leave out important details about how the data is actually processed and don't let people get a full picture of how their data is being used.

It can therefore be concluded that Meta does not sufficiently meet the transparency requirements under Art. 12–14 of the GDPR when it comes to training generative AI models.

3.5 Rights of data subjects (Art. 15–21 GDPR)

Meta's processing of data for AI training purposes raises significant issues regarding the protection of data subjects' rights under Art. 15 to 21 GDPR.

According to its own statements, Meta does provide an option to object to the use of personal data for AI training ("Submit an objection request"). However, there is no guarantee that such an objection will be implemented in full, both in terms of content and technology. In particular, it remains unclear how personal data that has not been published by the data subject themselves but by third parties – for example, in posts, comments, or images in which the data subject is recognizable – will be handled.

In such cases, an individual objection does not automatically prevent further processing of this content if it was posted by other users who have not themselves lodged an objection. This creates a real risk that, despite the objection, personal data will continue to be included in the training material or will be reused.

Furthermore, it remains unclear how Meta complies with the right to erasure under Article 17 GDPR, particularly with regard to models that have already been trained. Although the company states that deleted data will "not be used for future training," there is no comprehensible information on whether and how the data subject can verify that their data has actually been deleted and will no longer be used in future training processes. The handling of model parameters already derived from this data is also unclear, which is particularly problematic from a data protection perspective, as trained models do not allow selective deletion.

There are also significant shortcomings with regard to the right to information under Article 15 GDPR. It is not clear whether and to what extent Meta provides information on whether and how specific personal data has been incorporated into AI training processes – for example, with regard to origin, purpose of processing, scope, and recipients.

Overall, the rights of data subjects under Art. 15 to 21 GDPR are currently not effectively enforceable in the context of AI data processing by Meta. In particular, there are considerable doubts as to whether objections are fully taken into account, deletion obligations are properly fulfilled, and rights of access are comprehensively guaranteed. The fundamental rights of data subjects therefore remain unprotected in key areas.

3.6 Data protection impact assessment (DPIA, Art. 35 and 36 GDPR)

According to Article 35 GDPR, a data protection impact assessment (DPIA) must be carried out if a form of processing is likely to result in a high risk to the rights and freedoms of natural persons. This applies in particular to the systematic and extensive evaluation of personal characteristics using automated procedures and to the large-scale processing of special categories of personal data (Art. 35(3) GDPR).

In the present case, Meta processes personal data from several hundred million users, including sensitive information such as photos, posts, message metadata, and personal characteristics that can be derived from this data. The processing is automated, repeated, and carried out on a massive scale. It also includes data that has not been provided directly by the data subjects, such as through third-party posts, tagging, or public interactions.

The associated risks include loss of control over one's own data, opaque profiling, lack of transparency of model content, and potential discrimination through AI-generated outputs.

In addition, users cannot identify which specific data is affected and how it is reused. Even after an objection has been lodged or data has been deleted, there is a risk that trained models will continue to allow indirect conclusions to be drawn about the data originally processed.

This risk situation justifies the obligation to carry out a DPIA in accordance with Art. 35 GDPR. It must be prepared before processing begins, documented in writing, and regularly reviewed and updated. It is currently not apparent whether Meta has prepared or made publicly available such a DPIA. The absence of a verifiable DPIA constitutes an independent violation of the GDPR.

Nor is any consultation process with the competent supervisory authority pursuant to Art. 36 GDPR known. In the author's opinion, however, such consultation would have been legally mandatory due to the significant risk potential of the planned data processing.

In view of the nature, scope, circumstances, and purposes of the processing—in particular the large-scale, automated analysis of personal and, in some cases, sensitive data for the training of generative AI models—there is an obligation to carry out a data protection impact assessment in advance in accordance with Art. 35 GDPR. If this leads to the conclusion that, despite the planned protective measures, there remains a high risk to the rights and freedoms of the data subjects, Meta is obliged under Article 36 GDPR to consult the supervisory authority before commencing processing.

The lack of transparency regarding the relevant procedures, risk assessments, and coordination with the supervisory authority indicates a failure to comply with the obligations under Art. 35 and 36 GDPR.

4 Legal consequences

In the absence of a valid legal basis within the meaning of Art. 6 and 9 GDPR, Meta's planned use of personal content from Facebook and Instagram profiles for the development of generative AI models violates key provisions of the GDPR.

In addition, there are considerable doubts as to whether the legal requirements for transparency (Art. 12–14 GDPR), the protection of data subjects' rights (Art. 15–21 GDPR), and the performance of a data protection impact assessment (Art. 35 et seq. GDPR) are being complied with.

These violations give rise to the following legal consequences in particular:

4.1 Measures taken by supervisory authorities (Art. 58 and 83 GDPR))

The data protection supervisory authorities are authorized under Article 58(2) GDPR to order Meta to take a number of remedial measures. In the event of a serious breach such as the processing of personal social media data without an effective legal basis, as in the present case, the following measures are particularly relevant:

First, a prohibition of processing may be imposed (Art. 58 para. 2 f) GDPR). The supervisory authority may require Meta to cease processing the personal data concerned in whole or in part. In view of the scope of the planned AI processing, the sensitivity of the data concerned (in particular that covered by Art. 9 GDPR) and the lack of a legal basis, such a prohibition seems appropriate.

In addition, the authority may issue an order to delete data that has already been collected (Art. 58 (2) (g) GDPR). This applies not only to directly stored personal data, but may also extend to models derived from it – in particular if the training data remains traceable in the model parameters or can be reconstructed.

Finally, a fine may be imposed (Art. 58 (2) i) in conjunction with Art. 83 GDPR). The actual amount depends, among other things, on the severity, duration, intent, and likelihood of repetition. The GDPR provides for a maximum penalty of €20 million or 4% of global annual turnover, whichever is higher.

Based on Meta's annual turnover of approximately $135 billion in 2023, this results in a potential fine of up to approximately $5.4 billion.

4.2 Claims for damages by data subjects (Art. 82 GDPR)

Under Art. 82 GDPR, data subjects are entitled to compensation for both material and immaterial damage if their personal data is processed unlawfully. This requires a violation of the GDPR, resulting damage, and a causal link between the two.

The European Court of Justice has clarified that non-material damage – such as the loss of control over personal data, the feeling of constant surveillance or emotional impairment – is

also eligible for compensation.There is no threshold for materiality; even minor impairments can justify a claim for damages if they are substantiated.[7]

The amount of damages depends on the nature, scope, and sensitivity of the unlawfully processed data, the degree of fault on the part of the controller, and the scope of the data processing. In case law, amounts between 300 and 1,000 euros have already been awarded for comparatively minor infringements. In the event of serious infringements of personal rights, in particular in the processing of special categories of personal data pursuant to Art. 9 GDPR, significantly higher amounts may be considered in accordance with our legal opinion.

In the present case, the planned data processing by Meta does not only concern isolated pieces of information, but potentially complete digital profiles of several hundred million users. This includes the processing of particularly sensitive information such as political opinions, religious beliefs, health data, or information on sexual orientation—without a viable legal basis, in a non-transparent manner, and for an economically highly relevant purpose.

In German case law, amounts between EUR 25 and EUR 30,000 have been awarded, with the average amount of damages awarded being around EUR 3,300.[8]

In view of the high level of interference with personal rights, the systematic nature of the processing, and the particular sensitivity of the data concerned, damages in the lower to mid four-digit range—around EUR 5,000 per person—seem realistic.

Even if only one percent of the estimated 260 million people affected were to successfully assert such claims, this would result in a potential total liability risk in the double-digit billion range – an amount that would significantly exceed the level of fines permitted under Article 83 GDPR.

[7] CJEU, Judgment of 4 May 2023 – C-300/21

[8] Horn/Stegemann, article of 27 November 2024, available at https://rsw.beck.de/aktuell/daily/meldung/detail/immaterieller-schadensersatz-ds-gvo-scraping-urteil.

Simpliant Legal PartG mbB
Fasanenstr. 12
10623 Berlin
Deutschland

info@simpliant.eu