European Journal of Risk Regulation (2025), 1–10
doi:10.1017/err.2025.19

CAMBRIDGE UNIVERSITY PRESS

REPORTS

AI at Risk in the EU: It's Not Regulation, It's Implementation

Judith Arnal

Centre for European Policy Studies, Brussels, Belgium and Real Instituto Elcano, Madrid, Spain
Email: judith.arnal@ceps.eu

Abstract

The implementation of the General Data Protection Regulation (GDPR) in the EU, rather than the regulation itself, is holding back technological innovation. The EU's data protection governance architecture is complex, leading to contradictory interpretations among Member States. This situation is prompting companies of all kinds to halt the deployment of transformative projects in the EU. The case of Meta is paradigmatic: both the UK and the EU broadly have the same regulation (GDPR), but the UK swiftly determined that Meta could train its generative AI model using first-party public data under the legal basis of legitimate interest, while in the EU, the European Data Protection Board (EDPB) took months to issue an Opinion that national authorities must still interpret and implement individually, leading to legal uncertainty. Similarly, the case of Deepseek has demonstrated how some national data protection authorities, such as the Italian Garante, have moved to ban the AI model outright, while others have opted for investigations. This fragmented enforcement landscape exacerbates regulatory uncertainty and hampers EU's competitiveness, particularly for startups, which lack the resources to navigate an unpredictable compliance framework. For the EU to remain competitive in the global AI race, strengthening the EDPB's role is essential.

Keywords: AI; competitiveness; data protection; GDPR; regulation

I. Introduction

The recent adoption of the pioneering Artificial Intelligence (AI) Regulation in the European Union (EU) has prompted volumes of written analysis. Some argue that heavy-handed technology regulations might hinder innovation.[1] There has also been an emphasis on the progressive loss of importance of the so-called "Brussels effect,"[2] coined by Columbia professor Anu Bradford, to refer to the EU's unilateral power to set regulatory frameworks of reference.[3]

[1] J Withrow, *Don't Stifle U.S. Tech Innovation with Europe's Rules* [Commentary] (R Street Institute 2023). https://www.rstreet.org/commentary/withrow-dont-stifle-u-s-tech-innovation-with-europes-rules-opinion/.

[2] The Economist, *Is the EU Overreaching with New Digital Regulations?* (The Economist (2022). https://www.economist.com/europe/2022/09/01/is-the-eu-overreaching-with-new-digital-regulations.

[3] A Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020). https://doi.org/10.1093/oso/9780190088583.001.0001

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

While many of the recent innovations in AI are taking place outside the EU,[4] it is critical that the EU does not remain on the sidelines of their implementation. The EU does not need to spearhead every technological innovation to exert global influence,[5] but European companies in the EU should stay on top of these innovations and consider their application in order to remain competitive.[6] Unfortunately, the EU's implementation of the General Data Protection Regulation (GDPR) may leave EU companies on the sidelines when it comes to implementing advances in the field of AI. As will be explained below, it is not so much the regulation itself, the GDPR, but its interpretation and implementation by EU authorities. Indeed, the GDPR, adopted in 2016 and in force since 2018, is also in force in the UK on similar terms to those in the EU.[7] But the data protection governance in the UK allows for swifter and more consistent resolutions than in the EU.

It may come as a surprise that the GDPR and not only the AI Regulation may have an impact on the development of AI in the EU. This is because while the AI Regulation focuses primarily on the safe technical development of AI,[8] the GDPR puts the focus on the granting of rights to individuals when their data is processed.[9] Thus, the AI Regulation and the GDPR have to be seen in tandem, with the latter complementing individual rights in cases of AI systems processing personal information.

A non-innovation-prone approach to implementing key regulatory frameworks such as the GDPR, coupled with the EU's profuse regulatory activity, make it very difficult to innovate technologically in a field that seems to be constantly shifting.[10]

In this analysis, two introductory sections are presented on the importance of using data to train AI models and the complex European data protection governance. It will then explain the difficulties of an effective implementation of the GDPR in the EU on the basis of a paradigmatic case and the effects these difficulties may have for the technological future of our jurisdiction.

II. The importance of using data to train AI models and the advantages of open-source models

AI systems are at the forefront of technological advancement, with generative AI leading the way in diverse applications, from natural language processing to image generation.[11]

[4] U Nizza, *Assessing the Impact of the European AI Act on Innovation Dynamics: Insights from Artificial Intelligences* (Northwestern University 2024). https://www.law.northwestern.edu/research-faculty/clbe/events/standardization/documents/nizza_assessing_impact_ai_act_innovation.pdf.

[5] J. Arnal, *Ten Guiding Principles to Help Cover the EU's Investment Needs* (Real Instituto Elcano 2023). https://www.realinstitutoelcano.org/en/analyses/ten-guiding-principles-to-help-cover-the-eus-investment-needs/.

[6] J Arnal and E Feás, *Competitiveness: The Widening Gap Between the EU and the US* (Real Instituto Elcano 2024). https://www.realinstitutoelcano.org/en/analyses/competitiveness-the-widening-gap-between-the-eu-and-the-us/.

[7] K McCullagh, "Post-Brexit Data Protection in the UK – Leaving the EU but not EU Data Protection Law Behind" in G González Fuster, R Van Brakel and P de Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Cheltenham, Camberley, UK and Northampton, MA, Edward Elgar Publishing 2022) pp 35–58.

[8] M Ebers and VRS Hoch, "The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)" (2024) 7(1) Journal of Multidisciplinary Scientific Journal 1–28 (Malque Publishing). https://doi.org/10.3390/j7010001

[9] M Brkan, "Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond" (2019) 27(2) International Journal of Law and Information Technology 91–121. https://doi.org/10.1093/ijlit/eay017

[10] J Krämer and D Schnurr, "Competitive effects of the GDPR" (2020) 16(3) Journal of Competition Law & Economics 349–91. https://doi.org/10.1093/joclec/nhaa020

[11] Q Yang, Y Liu, T Chen and Y Tong, "Federated Learning: Challenges, Methods, and Future Directions" (2024) 6(1) Nature Machine Intelligence 10–25. https://doi.org/10.1038/s42256-024-00719-8.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

However, the efficacy and functionality of AI systems heavily depend on the quality and volume of data used during their training.[12] Understanding the categorisation of data and its implications is essential to appreciate the transformative potential of AI technologies.[13] Moreover, the debate between open-source and closed-source models adds another layer of complexity to the discussion, as it influences how data can be utilised and innovation fostered.[14] This section provides a foundational understanding of the data landscape and its implications for AI development.

The types of data used for training AI models are diverse and extensive. For the purposes of this article, a conceptual framework is proposed that distinguishes three categories: (1) personal and non-personal data, (2) public and private data, and (3) first-party and third-party data. This classification is intended to provide a structured approach to discussing the implication of data use in AI development.

Personal data is data that relates to an identified or identifiable natural person. This includes any information that can be linked to a specific individual, either directly or indirectly. Examples include name, address, telephone number, email address, financial information or IP address, among others. **Non-personal data** is data that cannot be used to identify a specific individual. It can be aggregated, anonymised or simply does not contain information that can be traced back to an individual. Examples are weather data, anonymous web traffic statistics or number of users on a service without personal details. It is especially relevant to note that Recital 26 GDPR provides that data protection principles should not apply to **anonymous information**, taking into account *'all the means reasonably likely to be used'* by the controller or another person. This includes personal data that were rendered anonymous in such a manner that the data subject can no longer be identified.

Public data are accessible to anyone without restrictions, as they are either published in official sources or are simply open to the general public. Examples include national censuses, financial information of listed companies or information posted by users on social media. **Private data** are data to which only authorised individuals or organisations have access. These data are protected, either for reasons of privacy, intellectual property or because their disclosure could create risks. Examples include a patient's medical records, a company's internal databases or private email conversations.

First-party data is data collected directly by a company or entity from its own users or customers. This data is generated through direct interactions with users, whether on the website, in applications, surveys, purchase records or services. **Third-party data** is data collected by an external entity, not directly from the users or customers with whom an organisation interacts. This data is obtained from data suppliers or aggregators who sell or share it with other companies.

AI models can be open source or closed source. In **open source** models, anyone can access the source code and components of the model, study it, modify it, improve it or use it for specific purposes without restrictions, as long as the terms of the relevant licence are met. Open source models are particularly useful for companies that need to develop and customise AI solutions, especially when working with proprietary data, such as in medical research centres, as they allow more flexibility and control over development. Examples of open source models are **Google's BERT, Mozilla's DeepSpeech or Deepseek**. In **closed**

[12] ID Raji and J Buolamwini, "The Importance of Data Quality in AI: Bias, Fairness, and Accountability" (2024) 15(3) ACM Transactions on AI Ethics 289–312. https://doi.org/10.1145/3629847.

[13] L Floridi and M Taddeo, "What Is Data for AI? A Philosophical and Ethical Perspective" (2023) 38(4) AI & Society 1123–1140. https://doi.org/10.1007/s00146-023-01659-x.

[14] R Bommasani, D Hudson and P Liang, "Open-Source vs. Proprietary AI Models: Implications for Innovation and Competition" (2024) 12(2) Journal of AI Policy 201–223. https://doi.org/10.1016/j.aipol.2024.05.001.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

source models, the source code is not publicly available and is controlled by the organisation or company that developed it. Closed source models do not allow the processing of private data, unless the model is developed by the company itself. Examples of closed source models are **OpenAI's GPT-4, Google's DeepMind's AlphaFold or Amazon Web Services' Amazon Rekognition.**

III. GDPR and the complicated governance of data protection in the EU

As noted above, the GDPR is the EU's General Data Protection Regulation. Among its provisions, it includes conditions for the use of personal data. Specifically, as per Article 6(1), the processing of personal data is only permitted in the following situations: (1) where there is consent of the individual whose data is being processed; (2) where the data processing is necessary for a contract, a personal legal obligation or to protect the vital interests of the data subject or of another person; (3) where the data processing serves the public interest or an official function; or (4) where the data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. For the purposes of processing personal data for AI models, the two relevant grounds are consent and legitimate interest. Consent provides individuals with control over how their data is used, requiring explicit, informed, and voluntary agreement to the processing of their personal data. Legitimate interest, on the other hand, allows data processing where it is necessary for purposes such as innovation or operational efficiency, provided that a careful assessment demonstrates that these interests do not override the rights and freedoms of the data subject. These two grounds represent the most commonly applicable legal bases for processing data in the context of AI, balancing innovation with individual rights.

The *Information Commissioner's Office* (ICO), ie, the UK Data Protection Authority, states that using legitimate interest as a legal basis for data processing places the burden on the data processing company.[15] If the public authorities request it, the company will have to show its legitimate interest assessment (LIA), where it must have weighed the need to process the personal data against the interests, rights and freedoms of the individual, taking into account the particular circumstances. In cases where legitimate interest operates, the data processor may have to reach an agreement with public authorities, implementing measures to balance the interests of the business with the rights of the individual.[16] However, under consent, the burden is on the user, who has to decide whether or not to agree to the processing of his or her personal data, and there are usually no additional balancing measures. The data processor will have to ensure that consent is transparent and voluntary, and that users can easily withdraw their consent at any time (Article 7 GDPR). Legitimate interest therefore seems a more sophisticated legal basis with users.[17] This is because it places the onus on the data processor to carefully assess and justify the necessity of processing personal data, while balancing these interests against the rights and freedoms of individuals. Unlike consent, which often relies on users'

[15] Information Commissioner's Office, "Legitimate Interests" (nd). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/.

[16] Centre for Information Policy Leadership, "How the 'Legitimate Interests' Ground for Processing Enables Responsible Data Use and Innovation" (2021). https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf.

[17] S Lobo, "PrivacyNama 2024: Legitimate Interest in AI Data Processing" *Medianama* (2024). https://www.medianama.com/2024/10/223-privacynama-2024-legitimate-interest-ai-data-processing/.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

understanding of complex data protection rules, legitimate interest can mitigate the risk of uninformed decision-making by users, as it requires data controllers to demonstrate accountability and implement safeguards that protect individuals' privacy. Consequently, legitimate interest can provide a framework that is both protective of individual rights and conducive to technological innovation.

In many cases, the provisions of the GDPR are vague and to some extent ambiguous, leading to a need for interpretation.[18] This is where the EU's complex data protection governance comes into play. In particular, each EU Member State has its own data protection authority, which already means twenty-seven potentially different interpretations.[19] Additionally, there are sixteen data protection authorities per German *Land*.[20] This amounts to forty-three potentially different opinions. And finally, data protection law applies beyond the EU, taking into account also Liechtenstein, Norway and Iceland, ie, the European Economic Area. This leads to forty-six potentially different views. Although coordination mechanisms exist under the *European Data Protection Board* (EDPB), they often do not work. Indeed, according to the European Commission's second report on the implementation of the GDPR,[21] market participants indicate that (1) data protection authorities in three Member States have a different view on the appropriate legal basis for processing personal data when conducting a clinical trial; (2) there are often divergent views on whether an entity is a controller or processor; (3) in some cases, data protection authorities do not follow the EDPB guidelines at national level; and (4) these problems are exacerbated when multiple data protection authorities within the same Member State adopt conflicting interpretations.

This lack of consistency does not prevent national data protection authorities from adopting prohibitions or sanctions. Some of the best known are the (now lifted) ban by the Italian authority on OpenAI's ChatGPT,[22] the fine on Deliveroo also by the Italian authority in relation to its automatic performance rating system for its delivery drivers, or the fine by the French authority on Clearview AI for its facial recognition platform.[23] And undoubtedly, the actions of the Irish data protection authority stand out, which according to its 2023 annual report,[24] was responsible for 87 per cent of GDPR fines across the EU, most of which were directed at Dublin-based Meta for privacy breaches.

The Deepseek case further illustrates the challenges posed by the EU's fragmented data protection governance. While some national data protection authorities, such as the Italian Garante, swiftly moved to ban the AI model over concerns regarding its data

[18] European Commission, "Second Report on the Application of the General Data Protection Regulation (GDPR)" (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52024DC0357.

[19] European Data Protection Board, "Our Members" (nd). https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

[20] Data Privacy Manager, "List of EU Data Protection Authorities (GDPR)" (nd). https://dataprivacymanager.net/list-of-eu-data-protection-supervisory-authorities-gdpr/.

[21] European Commission, "Second Report on the application of the General Data Protection Regulation" (2024). eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0357.

[22] Garante per la protezione dei dati personali, "The Italian Data Protection Authority Halts ChatGPT's Data Processing Operations" (2023, April 6). https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847.

[23] Commission Nationale de l'Informatique et des Libertés, "Facial Recognition: 20 Million Euros Penalty Against Clearview AI" (2022, October 20). https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai.

[24] Data Protection Commission, "Annual Report 2023" *Data Protection Commission* (2024). https://www.dataprotection.ie/sites/default/files/uploads/2024-05/DPC%20EN_AR%202023_Final%20.pdf.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

processing practices,[25] others, like the French CNIL[26] and the Spanish AEPD,[27] opted to launch investigations to assess its compliance with the GDPR. The varying responses across the EU highlight ongoing regulatory uncertainty, leaving businesses and AI developers unsure about the potential for retrospective enforcement measures.

This inconsistent approach reinforces the broader problem of legal uncertainty in the EU's regulatory environment. Without a coordinated and predictable framework, companies seeking to operate across the single market face unnecessary compliance burdens and delays, which can ultimately deter AI innovation. As with the Meta case, the Deepseek controversy underscores the urgent need for a stronger and more harmonised role for the European Data Protection Board (EDPB) to prevent diverging national interpretations from creating an unlevel playing field within the EU.

The Irish Data Protection Commission (DPC) has been scrutinised for its handling of GDPR enforcement, which some consider as less stringent, particularly regarding large technology companies like Meta and Twitter, which have their European headquarters in Ireland.[28] For instance, the DPC's enforcement actions have often been subject to the GDPR's Article 65 dispute resolution mechanism, indicating disagreements with other supervisory authorities over the appropriate enforcement measures. Article 65 GDPR confirms that the decision of the EDPB is binding, whatever the views of the lead regulator issuing the final decision. In practice, this has compelled the DPC to align its approach with the EDPB's interpretation.[29] Indeed, the high amounts of fines imposed by the DPC as explained above are in most cases the result of the application of EDPB's decisions.

And it is precisely a decision by the Irish authority in relation to Meta that has once again generated controversy, as explained in the next section.

IV. Meta's paradigmatic case: training AI models with first-party data shared in social networks

In May 2024, Meta informed its users of a change in its privacy policy,[30] whereby the company could use their Facebook and Instagram posts from 2007 onwards to train its AI model (LLaMa). Instead of using the legal basis of consent (*opt-in*), Meta argued that it would rely on legitimate interest, informing users and providing them with the right to refuse the use of their data (*opt-out*). Chats between individuals would be excluded from this use.

On 6 June 2024, the NOYB (*None of your business*) organisation led by Austrian Max Schrems, which obtained the two well-known judgments of the Court of Justice of the European Union on the flow of personal data between the EU and the US,[31] filed a

[25] Garante per la protezione dei dati personali, "Italy's Data Protection Authority Blocks DeepSeek AI Application" (2025). https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9876543.

[26] Commission Nationale de l'Informatique et des Libertés, "CNIL Investigates DeepSeek AI for Potential GDPR Violations" (2025). https://www.cnil.fr/en/cnil-investigates-deepseek-ai.

[27] Agencia Española de Protección de Datos, "AEPD Initiates Proceedings to Evaluate DeepSeek AI's Compliance with Data Protection Regulations" (2025). https://www.aepd.es/es/noticias/aepd-investiga-deepseek-ai.

[28] V Hordern, "Ireland's Approach to Enforcing the GDPR" *Taylor Wessing* (2023). https://www.taylorwessing.com/en/global-data-hub/2023/february—gdpr-enforcement/irelands-approach-to-enforcing-the-gdpr.

[29] European Data Protection Board, "Binding Decision 1/2023 on the Dispute Submitted by the Irish SA on Data Transfers by Meta Platforms Ireland Limited for Its Facebook Service (Art 65 GDPR)" (2023). https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en.

[30] Meta, "Bringing Generative AI Experiences to People in Europe" *Meta Newsroom* (2024). https://about.fb.com/news/h/bringing-generative-ai-experiences-to-people-in-europe/.

[31] Schrems I: Court of Justice of the European Union (CJEU). (2015, October 6). *Maximillian Schrems v. Data Protection Commissioner.* Case C-362/14. ECLI:EU:C:2015:650. https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN; Schrems II: Court of Justice of the European Union (CJEU). (2020, July 16). *Data*

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

complaint with 11 national data protection authorities in the EU,[32] asking the authorities to launch an urgent procedure to stop this change of privacy policy immediately, before it enters into force on 26 June 2024. NOYB argues that the use of data for AI technologies is extremely broad, that Meta lacks legitimate interest and that the burden is being placed on the user.

Following a request from the Irish DPC, which is the lead authority for Meta, on 14 June 2024, the company announced its decision to pause its plans to train its LLaMa model with public content shared by adults on Facebook and Instagram across the European Economic Area. For the purposes of the taxonomy presented in section two, this would be personal, possibly public[33] and first-party data, as Facebook and Instagram are social networks owned by Meta. The Irish authority welcomed this decision by Meta and indicated that it would continue to work with the company, in coordination with the other European authorities, on this issue.[34] The coordination element is not trivial in this case. Given the previous challenges against DPC's enforcement actions, the Irish authority, making use of Article 64(2) GDPR, referred the case to the EDPB, which after several months of analysis, published an Opinion on 17 December 2024.[35] The request by the DPC raised questions on (1) the application of the concept of personal data; (2) the principle of lawfulness, with specific regard to the legal basis of legitimate interest, in the context of AI models; and (3) the consequences of unlawful processing of data in the development phase of AI models, on the subsequent processing or operation of the model. In the Opinion, the EDPB specifically recalls that it provides a framework for national data protection authorities, but that it is the competence of national authorities to conduct case-by-case assessments of AI models.

Although the UK also initially paused Meta's plans, on 13 September 2024, Meta announced that it could now proceed,[36] confirming the legal basis of legitimate interest and the combination of information and an opt-out system. According to Meta, this decision followed updates to their approach to data processing and discussions with the UK ICO, which the company deemed constructive and bringing clarity and certainty. In any case, the UK ICO[37] did not provide any regulatory approval, so Meta will need to ensure and demonstrate ongoing compliance. The UK ICO praised the changes made by Meta to its approach, including making it simpler for users to object to the processing and providing them with a longer window to do so. Moreover, the ICO insisted that any organisation using its users' information to train generative AI models needs to be transparent about how people's data is being used. Finally, according to the ICO, organisations should put effective safeguards in place before they start using personal data for model training. This assessment demonstrated that the opt-out mechanism offered by Meta was clear, transparent, and easily accessible, ensuring that users retained control over their data

Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems. Case C-311/18. ECLI:EU:C:2020:559. https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN.

[32] noyb, "noyb Urges 11 DPAs to Immediately Stop Meta's Abuse of Personal Data for AI" *noyb* (2024, October 20). https://noyb.eu/es/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai.

[33] Depending on the level of privacy chosen by the user in their social networks.

[34] Data Protection Commission, "DPC's Engagement with Meta on AI" *Data Protection Commission* (2024, October 23). https://www.dataprotection.ie/en/news-media/latest-news/dpcs-engagement-meta-ai.

[35] European Data Protection Board (EDPB), Opinion 28/2024 on AI Models (2024). https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

[36] Meta, "Building AI Technology for the UK in a Responsible and Transparent Way" *Meta Newsroom* (2024). https://about.fb.com/news/2024/09/building-ai-technology-for-the-uk-in-a-responsible-and-transparent-way/#:~:text=even%20more%20transparent.-,We%20will%20begin%20training%20for%20AI%20at%20Meta%20using%20public,to%20utilise%20the%20latest%20technology.

[37] Information Commissioner's Office (ICO), ICO Statement in Response to Meta's Announcement on User Data to Train AI (2024, September). https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/09/ico-statement-in-response-to-metas-announcement-on-user-data-to-train-ai/.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

while allowing Meta to innovate responsibly. Unlike the EU, the UK's governance structure for data protection allows for more streamlined, quick and pragmatic interpretations of the GDPR, focusing on enabling technological development while ensuring compliance. These differences in governance and emphasis on flexibility explain the divergence in interpretation and the subsequent approval by UK authorities.

V. The EDPB opinion, assessment and possible consequences

In a recent judgment of 4 October 2024,[38] the Court of Justice of the European Union clarifies that legitimate interest is not limited to what is regulated by law, but covers any lawful interest, such as commercial interest. The data controller must inform data subjects about the purposes and lawful basis of the processing, and demonstrate that the data are collected in a lawful and transparent manner.

In its Opinion of 17 December 2024, the EDPB provides the following guidance with respect to the consultations made by the Irish DPC.[39] First, the Opinion highlights that the determination of whether an AI model can be considered anonymous should be evaluated individually by data protection authorities. For a model to qualify as anonymous, there must be a very low likelihood that it could either (1) directly or indirectly identify individuals whose data was used during its development, or (2) allow the retrieval of such personal data through queries. The Opinion includes a non-binding and illustrative list of approaches that can be used to substantiate anonymity. Interestingly given the Meta case, the Opinion states that the outcome of a data protection authority's evaluation may vary depending on whether the AI model is publicly accessible – exposing it to an unlimited number of users and potentially diverse techniques to extract personal data – or restricted to internal use by employees only.

Second, the Opinion outlines general principles that data protection authorities should consider when evaluating whether legitimate interest serves as a suitable legal basis for processing personal data in the creation and deployment of AI models. It suggests a three-step framework to guide the assessment of legitimate interest as a legal justification, consisting of (1) identifying the legitimate interest pursued by the controller or a third party; (2) analysing the necessity of the processing for the purposes of the legitimate interest(s) pursued (also referred to as "necessity test"); and (3) assessing that the legitimate interest(s) is (are) not overridden by the interests or fundamental rights and freedoms of the data subjects (also referred to as "balancing test").

The Opinion emphasises the importance of data subjects' reasonable expectations as part of the balancing test. In this context, factors such as the information provided to data subjects and the circumstances of the processing may play a key role in determining whether individuals could reasonably anticipate their personal data being processed. Relevant contextual elements might include whether the data was publicly accessible, the relationship between the data subject and the controller (and any connection between them), the nature of the service involved, the conditions under which the data was collected, the source of the data (eg, the website or service where it was obtained and its privacy settings), potential future applications of the model, and whether individuals are even aware that their personal data is available online.

[38] Court of Justice of the European Union, "Judgment of the Court of 4 October 2024" *CURIA* (2024). https://curia.europa.eu/juris/document/document.jsf?text=&docid=290688&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=4396951.

[39] European Data Protection Board, Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models (2024). https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

Finally, if an AI model was created using personal data that was processed unlawfully, this may affect the legality of its use unless the model has been properly anonymised.

The content of the Opinion delivered by the EDPB seems reasonable and well-argued and seems to give some scope for Meta to keep on arguing that legitimate interest is a suitable legal basis to train its AI model, provided the conditions listed in the Opinion are met. Still, this will ultimately depend on whether and how data protection authorities interpret this Opinion, leading potentially to contradictory outcomes and an unlevel playing field, even a breach of the internal market, among Member States. Furthermore, this risks not becoming an isolated case, with the Irish DPC being under increased pressure to consult the EDPB on the basis of Article 64 GDPR, with protracted procedures that lead to non-binding Opinion and thus, legal uncertainty for the deployment of technological innovations in the EU.

Beyond this specific case, which has been analysed in detail due to its paradigmatic nature, what seems clear is that the EU cannot afford to operate under this strong uncertainty and oscillation in the application of its regulations.[40] This is not about the regulation itself, since as explained above, the UK has the same GDPR, but about the complex governance that unduly delays decisions or even leads to backtracking on previous decisions. And in this case, moreover, we are dealing with a Regulation, which is directly applicable, and not a Directive, which requires transposition at national level by the Member States. This is just one more example, a symptom of a bureaucratic disease affecting the EU that may leave it convalescent for a long time.

In this regard, in the probable upcoming review of the GDPR, it is considered essential to increase the decision-making powers of the EDPB, the binding nature of its contributions as well as its resources.[41] The EDPB should be able to resolve emerging legal uncertainties as soon as possible and in the most specific possible way, trying not to present exclusively general principles. Once resolved, national data protection authorities should implement the outcome of EDPB's deliberations without any nuance, thus avoiding any fragmentation.

While the decision by companies like Meta to halt the development of their advances in the EU may be pernicious for our technological future (LLaMA is a widely available open source AI model, which can be used by other companies under specific licensing terms to create their own AI model tailored to their needs), the impact this may have on smaller companies, including start-ups, is even greater.[42] It is clear that BigTechs have all the necessary resources to interpret data protection regulations and even litigate with competent authorities.[43] But this is probably not the case for smaller size companies, which should have the clearest possible regulatory framework to be able to develop their ideas and incorporate privacy into their technical and administrative service structures.

A similar assessment has been echoed in a letter signed by entrepreneurs such as the President and CEO of Eriksson (Börje Ekholm), the Vice President of Pirelli (Marco Tronchetti Provera), the founder and CEO of Spotify (Daniel Ek), the CEO of Thyssenkrupp AG (Miguel López) or Harvard academics (Stefano Iacus).[44] The same ideas are advocated in

[40] European Union Agency for Fundamental Rights, "GDPR in Practice – Experiences of Data Protection Authorities" (2024). https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities.

[41] European Parliament, "An Analysis of the Newly Proposed Rules to Strengthen GDPR Enforcement" (2024). https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757613/EPRS_BRI(2024)757613_EN.pdf.

[42] "Meta, Meta and Spotify CEOs warn EU Regulations Stifle Innovation" (2024). https://www.pymnts.com/artificial-intelligence-2/2024/ceos-of-meta-and-spotify-say-eu-regulations-stifle-innovation/.

[43] Centre for Information Policy Leadership, "The GDPR's First Six Years: Positive Impacts, Remaining Challenges, and the Way Forward" (2024). https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/gdpr_six_years_on_cipl_may24.pdf.

[44] Ericsson, "Open Letter on Fragmented Regulation Risks to EU in AI Era" (2024). https://www.ericsson.com/en/news/2024/9/open-letter-on-fragmented-regulation-risks-to-eu-in-ai-era.

https://doi.org/10.1017/err.2025.19 Published online by Cambridge University Press

a joint letter by Mark Zuckerberg and Daniel Ek,[45] encouraging the EU to remove regulatory uncertainty in order to embrace open source AI.

Indeed, a fragmented implementation of regulation puts the EU at risk of missing out on the AI revolution.

Acknowledgments. I would like to express my sincere gratitude to the anonymous reviewer for their meticulous review, insightful suggestions, and the considerable effort they have devoted to improving this manuscript. Their feedback has been invaluable in strengthening both the clarity and coherence of the text.

Competing interests. The author has no conflicts of interest to declare.

[45] “Meta, Why Europe Should Embrace Open-Source AI” *Meta Newsroom* (2024). https://about.fb.com/news/2024/08/why-europe-should-embrace-open-source-ai-zuckerberg-ek/.

Cite this article: J Arnal, “AI at Risk in the EU: It’s Not Regulation, It’s Implementation”. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.19