Jean Monnet Network on EU Law Enforcement

Working Paper Series

Conference:

'The many faces and facets of the enforcement of European Union law: adapting in the ever-evolving landscape and empowering change for successful policies'.

11-12 December 2025, Utrecht University

SHOULD DATA PROTECTION AUTHORITIES ENFORCE THE *AI ACT*?

LESSONS FROM EU-WIDE ENFORCEMENT DATA

Joanna Mazur[*] Claudio Novelli[†] Zuzanna Choińska[‡]

Abstract: Most Artificial Intelligence (AI) systems involve some form of personal data processing, yet the role of Data Protection Authorities (DPAs) in enforcing the *AI Act* remains critically undefined. This article empirically investigates the current scope of DPAs' activities in enforcing regulations concerning AI-driven services and automated decision-making (ADM) systems to assess their suitability for enforcing the *AI Act*. Drawing on a dataset covering DPA activities relating to AI in all European Union Member States, we analyse multiple indicators as proxies for their activity level concerning enforcement related to AI and ADM. Our findings suggest that, although many DPAs have some experience with AI-related enforcement, their activity level in this area varies significantly. Combining these results with a legal analysis of the *AI Act*'s provisions, we argue that, despite being heterogeneous, the expertise developed by DPAs represents a valuable resource for effectively enforcing the *AI Act*.

Keywords: Artificial Intelligence, *AI Act*, automated-decision making, Data Protection Authorities, enforcement, right to explanation

[*] University of Warsaw, joanna.mazur@uw.edu.pl. This research (Joanna Mazur and Zuzanna Choińska) is supported by the research grant of the National Science Centre, Poland (grant number 2024/53/B/HS5/00169). This paper has been previously made available on SSRN: https://ssrn.com/abstract=5290513 and Zenodo: https://zenodo.org/records/15646626 (both text and dataset). Please, note that it is a preprint version.
[†] Yale University, claudio.novelli@yale.edu.
[‡] University of Warsaw, z.choinska@delab.uw.edu.pl.

I. INTRODUCTION

Artificial Intelligence (AI) technologies often rely on processing personal data. However, the role of Data Protection Authorities (DPAs) within the enforcement model of the *AI Act*[4] remains unclear. This article investigates how actively DPAs currently enforce data protection rules in cases concerning AI-based products and services and automated decision-making (ADM) systems. Drawing on evidence from documented DPA activities across EU Member States, we develop an index to quantify their activity level, identifying concrete ways they could contribute to effectively enforcing the *AI Act*. Our analysis specifically addresses explicitly three key research questions: two descriptive (1 and 2) and one prescriptive (3):

1) What role does the *AI Act* assign to DPAs within its enforcement model?

2) What is the current DPAs' activity level in relation to AI-driven products or services and ADM systems?

3) Given their experience, how *should* DPAs be involved in enforcing the *AI Act*?

We address these questions through an empirical legal study. Section II presents the *AI Act*'s provisions regarding the potential involvement of the DPAs in its enforcement. Section III describes the methods and sources used for the empirical analysis, while Section IV presents the results. For the empirical analysis, we collected and analysed a unique dataset on the activities of DPAs across all EU Member States, structured by the following indicators: (1) data protection impact assessment (DPIA) blacklist inclusions (with explicit or implicit references to AI); (2) AI-related decisions; (3) ADM-specific decisions (concerning Article 22 of the General Data Protection Regulation — GDPR[5]); (4) mentions of AI in annual reports (2021–2024); and (5) website search results for search terms describing AI. We decided to include the decisions concerning ADM for two reasons. We chose to include decisions concerning ADM for two reasons. Firstly, as we explain below, the AI Act includes a right resembling the right to explanation under the GDPR. Secondly, experience in the enforcement of ADM is essential for the enforcement of many high-risk AI systems under the *AI Act*, as these systems often entail processing personal data and ADM. Therefore, alongside the indicators directly referring to AI, we also include those concerning ADM.

The results of this analysis are used to evaluate the activities that the DPAs have undertaken in relation to AI-related matters. We treat the collected data as a proxy for assessing the readiness of DPAs to enforce legal norms in AI- and ADM-related cases. This assessment proposes a quantitative index based on the indicators mentioned above. Member States are then divided into four groups according to their activity level: very active, active, reluctant and inert enforcers. We then discuss the characteristics of each group. Section V presents the results of the empirical analysis of the regulatory framework of the *AI Act*'s enforcement model. Assuming that a higher level of AI-specific enforcement activity indicates greater institutional learning and a stronger foundation for effective future enforcement, we propose evidence-based solutions for the scope of DPAs' involvement in the *AI Act*'s enforcement system.

Based on this analysis, we have three targeted recommendations. Firstly, given their experience with ADM-related oversight, DPAs should be designated as the competent authorities under Article 86 of the *AI Act*, which guarantees individuals the right to an explanation in high-risk AI contexts. Secondly, we advocate including DPAs as Market Surveillance Authorities (MSAs) for high-risk AI systems under Annex III, points 3 to 5 of the *AI Act*, where the intersection of data protection and AI regulation is most evident. While very active and active enforcers could fulfil the role of MSAs, given their activity level, there might be doubts concerning reluctant and inert enforcers. In their case, we suggest that supranational cooperation could play a role in equipping them with the necessary resources for more active AI enforcement. Additionally, based on our data collection experience for this study, we advocate for establishing an EU-wide database of DPA decisions to enhance transparency and consistency within the decentralised enforcement framework shared by the GDPR

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ 2024 L 1689.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

and the *AI Act*. This database would also provide policymakers and researchers with reliable evidence for tracking enforcement trends and assessing supervisory performance.

II. THE ROLE(S) OF DPAS IN THE ENFORCEMENT SYSTEM OF THE *AI ACT*

The enforcement system of the *AI Act* is complex and still evolving. Its success hinges on a robust governance framework[6] — one that is uniform, well-coordinated, and adequately funded. The powers and responsibilities of the various institutional bodies established or implicated by the *AI Act* must be clearly defined to achieve this. Much of this clarification is still pending and will be established through the European Commission's implementing acts and the individual decisions of Member States.

In this context, our goal is to evaluate the potential role of DPAs within the governance structure established by the *AI Act*. To perform this assessment comprehensively, we must examine two key sources: the text of the *AI Act* itself and the statement issued by the European Data Protection Board (EDPB) concerning DPAs' responsibilities under the *AI Act* (Statement 3/2024).[7]

As previously mentioned, the governance structure outlined in the *AI Act* grants individual Member States a significant degree of autonomy. This allows considerable flexibility in assigning responsibilities for implementing and enforcing the *AI Act*, either to existing national authorities such as DPAs or new bodies. At the national governance level, Member States can create dedicated agencies or expand the mandates of existing entities, including DPAs. Given their existing mandate to protect fundamental rights, particularly privacy and data protection, extending the roles of DPAs would be a natural choice in the context of emerging technological developments.

Several provisions in the finalised text of the *AI Act* explicitly define, or at any rate suggest, the roles and responsibilities of DPAs as national competent authorities within its regulatory framework. DPAs are generally expected to assume supervisory and enforcement roles for specific high-risk AI systems. They are also expected to collaborate closely with the newly established AI-focused regulatory bodies to ensure that AI regulations align with existing data protection standards.

More specifically, the *AI Act* requires Member States to designate MSAs to oversee the compliance of AI systems — particularly high-risk ones — with established safety, health and fundamental rights standards.[8] To facilitate this supervisory role, the MSAs are empowered to access technical documentation, source code, and personal data where relevant, to verify compliance.[9] Crucially, the *AI Act* states that, for AI systems with significant implications for fundamental rights — such as those used in law enforcement, border control and immigration management[10] — the appointed MSA should be the national DPA or an equivalently independent body. Article 74(8) references explicitly Articles 41–44 of the Law Enforcement Directive,[11] effectively requiring any authority other than the DPA to be appointed to these roles to possess independence and comparable powers to those of a DPA.

Notably, the *AI Act* equips DPAs with investigatory powers beyond their traditional GDPR mandate. While Article 58 of the GDPR already allows DPAs to enter premises and request information from controllers or processors, the *AI Act* now empowers a DPA acting as an MSA to compel the disclosure of an AI system's

---

[6] Claudio Novelli, Philipp Hacker, Jessica Morley, Jarle Trondal and Luciano Floridi, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) *European Journal of Risk Regulation* 1, https://doi.org/10.1017/err.2024.57.

[7] EDPB, *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework* (Statement 3/2024) (16 July 2024) <https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf> accessed 9 June 2025.

[8] See *AI Act*, Art 70.

[9] See *AI Act*, Art 77.

[10] See *AI Act*, Art 74.

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), OJ 2016 L119/89.

training and testing datasets, detailed data-governance documentation, and, where strictly necessary, its source code. This capacity to inspect the model's 'black box' is intended to verify compliance with the *AI Act*'s requirements on data quality, robustness, transparency, and the absence of prohibited bias. Consequently, when a DPA is designated as the competent authority for a high-risk AI category, its remit encompasses the entire supervisory cycle: assessing providers' ex ante obligations (risk management, dataset and record-keeping controls, transparency measures); receiving and handling incident or non-compliance notifications; conducting inspections, audits, and functional testing of AI systems in operation; and ordering corrective measures or imposing administrative sanctions when breaches are identified.

Next, Article 86 of the *AI Act* gives users affected by decisions made by high-risk AI systems the right to ask the deployer for clear and meaningful explanations about the role of the AI system in the decision-making process.[12] The *AI Act* does not explicitly assign DPAs supervisory competence over this right. Still, they may play a role in its enforcement. This is because they may be designated as MSAs, there is an overlap with rights under the GDPR, and they have established mandates and expertise in data protection. This enables them to oversee compliance with both data protection and AI regulations.

Furthermore, the *AI Act* establishes specific notification obligations towards DPAs. For instance, when law enforcement authorities are permitted to use real-time or post-remote biometric identification systems in public, which is otherwise prohibited, the *AI Act* stipulates that each instance of such usage must be logged and made accessible to the relevant MSA and national DPA upon request. Deployers of these systems must also submit an annual report to the DPA.[13]

Similarly, DPAs serve as gatekeepers for processing personal data in regulatory sandboxes. Before a sandbox can be authorised, the relevant DPA must be consulted and may impose specific privacy and security conditions to ensure compliance with EU data protection rules.[14]

Article 74(9) at the EU level similarly designates the European Data Protection Supervisor (EDPS) as the MSA for AI systems deployed by EU institutions and agencies.

In addition to formally designated AI supervisors, the *AI Act* also empowers various 'authorities protecting fundamental rights'[15] — a category that, in the case of most Member States, includes DPAs[16] — to support enforcement. Article 77(1) states that any national body which enforces EU laws protecting fundamental rights in the context of the use of high-risk AI systems and which has been previously designated by Member States in a publicly available list can request and access documentation relating to AI systems created under the *AI Act* whenever necessary to fulfil its mandate. In other words, if a DPA or similar body is investigating a potential rights violation involving an AI system, it has the legal right to obtain the AI provider's technical file, logs, and any other documentation required for *AI Act* compliance. Importantly, the authority must inform the MSA of such requests, but does not require their permission. If the documentation alone is insufficient to assess a suspected rights infringement, Article 77(3) allows the fundamental rights authority (e.g., a DPA) to request that the MSA conduct testing or audit the AI system in question.

Overall, the AI Act gives DPAs considerable scope to act as national competent authorities, responsible for notification duties, market surveillance, and safeguarding fundamental rights. The competencies envisaged for DPAs build on their GDPR mandate, yet they extend well beyond it. However, it is essential to note that this appointment is not automatic: each Member State retains the discretion to decide which body will serve as the MSA, meaning that designating the DPA remains optional.[17]

---

[12] For a working paper on this topic, see Margot E Kaminski and Gianclaudio Malgieri, 'The Right to Explanation in the AI Act' (2025) *U of Colorado Law Legal Studies Research Paper No. 25-9*, <https://ssrn.com/abstract=5194301> accessed 31 May 2025.
[13] See *AI Act*, Art 26(10).
[14] See *AI Act*, Art 57(10) and 59(1).
[15] See *AI Act*, Art 77.
[16] See Digibeetle, 'List of authorities protecting fundamental rights (Article 77 AI Act)' (12 March 2025) <https://www.linkedin.com/posts/jbagerritsen_digibeetles-list-of-art-77-ai-act-authorities-activity-7305605824750493708-A5Oq?utm_source=share&utm_medium=member_desktop&rcm=ACoAACDTwaQBHkcKWW9-dGRe5PzeeYkZA-DbjaI> accessed 19 May 2025.
[17] See *AI Act*, Art 3(48).

Amidst this discretion, the EDPB urged governments to appoint DPAs as the MSAs for high-risk AI systems in *Statement 3/2024* of 16 July 2024. The EDPB characterises DPAs as the 'natural interlocutor' given that the *AI Act* aligns with EU data protection instruments, including the GDPR, the Law Enforcement Directive, and the ePrivacy Directive.[18] *Statement 3/2024* also suggests that a DPA should be the single point of contact for the public and cross-border cooperation at both the Member State and EU levels when assuming the MSA role.[19]

Although the EDPB's recommendation is influential, it is not legally binding, and Member States remain free to appoint an alternative body. The EDPB's reasoning is based on the practical experience that DPAs have gained in drafting guidance, shaping best practices, and enforcing AI-related data protection requirements. As explained in *Statement 3/2024*: 'DPAs have proven — and are still proving — to be indispensable actors in the chain leading to the safe, rights-oriented and secure deployment of AI systems across several sectors.'[20]

This is precisely the proposition we aim to test empirically in this article. In other words: do DPAs have the necessary expertise to enforce the *AI Act* effectively?

III. METHODS AND SOURCES

Data Collection

For the purposes of this study, we created a dataset capturing the various AI-related activities of DPAs across all Member States.[21] Our goal was to provide specific proxies for assessing the activity level of DPAs in handling AI-related cases or issues that may be important under the *AI Act*, such as ADM. Therefore, we collected data on the following indicators:

Indicator	Abbreviation	Description
Presence of the term 'AI' on national blacklists of processing operations requiring a data protection impact assessment (DPIA)	(1) DPIA blacklist inclusions	Verified on the basis of national DPIA blacklists. We also consider the possibility that AI may not be mentioned directly in the list, but that services or products using AI may still be subject to the DPIA (see Table 2).
Presence of decisions and opinions issued by DPAs concerning AI-based services or products	(2) AI-related decisions	We checked whether the databases containing decisions made by the DPAs included results relating to AI.
Presence of decisions and opinions that specifically address ADM	(3) ADM-specific decisions	We checked whether the databases that collect decisions made by DPAs contained any results relating to ADM. We used the official translation of the GDPR text to identify the relevant decisions or article numbers (Article 22), as this article is also mentioned in the content of other articles in the GDPR that refer to ADM. Therefore, the search should also allow us to identify decisions concerning other provisions. Using the relevant article numbers was

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (ePrivacy directive), OJ 2002 L 201/37.
[19] See *Statement 3/2024*, points 9–10.
[20] *Statement 3/2024*, point 6.
[21] Joanna Mazur, Claudio Novelli, and Zuzanna Choińska, '[dataset] Should DPAs Enforce the AI Act – Data on DPAs Activities in Relation to AI' (12 June 2025, Zenodo), <https://doi.org/10.5281/zenodo.15646626> accessed 12 June 2025.

		intended to increase the reliability of the collected data.
Presence of AI-related activities in DPAs' annual reports	(4) Mentions in annual reports	We collected information on whether the annual reports referred to AI. Data was collected for the years 2021, 2022 and 2023, as well as for 2024 where available, in order to capture how the DPAs have reacted to the rapid changes in the availability of generative AI technologies since 2022.
Number of search results relating to AI on the official websites of DPAs	(5) Website search results	We collected data on the results obtained by using the search function on each DPA's website. We used the phrase 'artificial intelligence' as the search term in the official language of the relevant DPA, as it appears in the translation of the *AI Act* into that language. Where necessary due to noun and adjective declension in the given language, we excluded the specific ending.

Table 1: The types of data collected in the study.

We use automated translation tools to collect information on these indicators for all Member States. Data collection took place from March to April 2025. Therefore, reports for 2024 were available only for some Member States.

There are numerous challenges in conducting this type of study. Firstly, we attempted to collect the enumerated data types for the enforcers at the regional level. Therefore, the total number of DPAs examined should include 27 DPAs from the Member States, 16 land DPAs in Germany, and three regional DPAs in Spain. Although the analysis focused on national institutions responsible for enforcement, including regional DPAs, it increased the reliability of the results for these countries.

Secondly, although automated translation is instrumental in this regard, linguistic challenges still pose a valid obstacle to finding relevant information. Therefore, we designed our indicators to confirm whether the DPA had issued a decision concerning AI or ADM, provided that we found at least one relevant result (see the next section). Our focus on enforcement practice justifies this approach,[22] as opposed to formal analyses of ADM regulation,[23] and by our objective of covering all Member States.[24] Although we cannot claim to have identified all the relevant decisions and opinions on this topic, we have compiled the most comprehensive dataset to date, containing information on the activities of DPAs concerning AI and ADM.

[22] For such a focus, see Ljubiša Metikoš and Jef Ausloos, 'The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act' (2025) 17(1) *Law, Innovation and Technology* 205.

[23] See, among others, Sandra Wachter, Brendt Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76; Andrew D Selbst and Julia Powles, 'Meaningful information and the right to explanation' (2017) 7(4) *International Data Privacy Law* 233; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7(4) *International Data Privacy Law* 243; Maja 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; Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 *Berkeley Technology Law Journal* 189.

[24] See Gianclaudio Malgieri, 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations' (2019) 35(5) *Computer Law & Security Review* 105327. For other attempts to conduct such studies comparing the enforcement of the GDPR in all Member States, see Ido Sivan-Sevilla, 'Varieties of Enforcement Strategies Post-GDPR: A Fuzzy-Set Qualitative Comparative Analysis (fsQCA) across Data Protection Authorities' (2022) 31(2) *Journal of European Public Policy* 552; Jukka Ruohonen and Kalle Hjerppe, 'The GDPR enforcement fines at a glance' (2022) 106 *Information Systems* 101876; Livia Puljak, Anamaria Mladinić and Zvonimir Koporc, 'Workload and procedures used by European data protection authorities related to personal data protection: a cross-sectional study' (2023) 16(41) *BMC Res Notes* 1.

Thirdly, it is worth noting that the DPAs employ different approaches to publishing their decisions and the parameters included in the search form. This is particularly problematic in the case of DPAs that publish non-searchable PDF files of their choices or that do not provide a search function covering the content of the decisions on their website. Some websites also have imprecise built-in search engines. Therefore, we had to consider these technical limitations when collecting data and developing indicators that would enable us to make comparisons involving all Member States despite discrepancies in access to their decisions, opinions, and information on their activities.

Due to these challenges, it was occasionally necessary to supplement the search with additional steps despite our efforts to minimise divergence from the aforementioned data collection template. For instance, we used the number of relevant articles in conjunction with the key terms. In some cases, due to a lack of access to DPAs' decisions, we focused on searching for relevant case law.[25] Furthermore, to improve the quality of the data collected, we compared our findings with the results of searches on GDPRhub,[26] Enforcement Tracker,[27] and GDPRxiv,[28] as well as with knowledge from relevant literature.[29] While these sources do not compile all the decisions issued by the DPAs, they enabled us to verify whether we had collected the decisions included in this database and to add those we had not previously identified. This increased the reliability of the results.

Data Analysis

The collected data is used as a proxy to assess the activity level of specific DPAs regarding the enforcement of AI and ADM. The following criteria were adopted for the analysis of this data:

Indicator	Scale	Score	Criteria
DPIA blacklist inclusions (B)	0–1	0	No national DPIA blacklist
		0.5	Although AI is not mentioned directly in the blacklist, products or services based on AI may be subject to a DPIA.
		0.75	Although AI is not mentioned directly in the blacklist, it is referenced in the DPIA description.
		1	AI is mentioned directly in the blacklist.[30]

[25] In the case of Germany and Austria.

[26] We used the results of the advanced search based on the relevant provisions (Arts 22, 13(2)(f), 14(2)(g), and 15(1)(h) and for the term 'artificial intelligence.' We performed the search on the 17th of March 2025 on GDPRHub, <https://gdprhub.eu/index.php?title=Advanced_Search>, accessed 28 April 2025.

[27] Search of the infringement of Article 22 on GDPR Enforcement Tracker, <https://enforcementtracker.com/>, accessed 28 April 2025.

[28] Search of the infringement of Article 22 on GDPxiv, <https://gdprxiv.org/>, accessed 28 May 2025. See also, Chen Sun et al., 'GDPRxiv: Establishing the State of the Art in GDPR Enforcement' (2023) 4 *Proceedings on Privacy Enhancing Technologies* 484.

[29] E.g., the proceedings against Clearview AI, see Joanna Mazur and Zuzanna Choińska, 'European Union data protection law and the use of facial recognition technology for the purpose of fighting crime,' in Michał Balcerzak and Julia Kapelańska-Pręgowska (eds), *Artificial Intelligence and International Human Rights Law* (Edward Elgar Publishing 2024) 124–144, and the cases invoked in the article Ljubiša Metikoš and Jeff Ausloos (n 22). For very inspiring in-depth empirical work concerning one Member State, see Laura Bachňáková Rózenfeldová et al., 'Personal Data Protection Enforcement under GDPR — the Slovak Experience' (2024) 14(3) *International Data Privacy Law* 278.

[30] See Joanna Mazur, 'Artificial Intelligence vs Data Protection: How the GDPR Can Help to Develop a Precautionary Regulatory Approach to AI?', in Angelos Kornilakis, Georgios Nouskalis, Vassilis Pergantis and Themistoklis Tzimas (eds) *Artificial Intelligence and Normative Challenges (Law, Governance and Technology Series, vol 59)* (Springer 2023) 215–223. The chapter elaborates on the argument that the use of AI may be subject to an obligatory DPIA under the

AI-related decisions (D_{AI})	0–1	0	No identified decisions or opinions.
		0.5	One identified decision or opinion.
		1	There is more than one identified decision or opinion of the DPA regarding AI-based services or products.
ADM-specific decisions (D_{ADM})	0–1	0	No identified decisions or opinions.
		0.5	One identified decision or opinion.
		1	There is more than one identified decision or opinion of the DPA regarding ADM.
Mentions in annual reports (R)	0–1	0	No mentions in any of the reports
		0.25	Mentioned in one report from the last four years.
		0.5	Mentioned in two reports from the last four years.
		0.75	Mentioned in three or more reports from the last four years.
		+0.25	An additional 0.25 points are awarded for reports containing separate chapters, sections or in-depth analyses of issues related to AI.
Website search results (W)	0–1	0	No mentions of AI on the website or no search function on the website
		0.25	There are 1–19 mentions of AI on the website.
		0.5	There are 20–99 mentions of AI on the website.
		0.75	There are 100 and more mentions of AI on the website.
		+0.25	An additional 0.25 points are awarded for separate web pages, FAQs, guidelines or statements relating to AI.

Table 2: The scores assigned to the results in relation to the specific indicators.

Next, we created an index that considers the varying weights of these indicators when evaluating the activity level of the DPAs regarding the enforcement of AI-related issues. The weights assigned to the particular indicators are as follows: DPIA blacklist inclusions (B) = 0.2; AI-related decisions (D_{AI}) = 0.25; ADM-specific decisions (D_{ADM}) = 0.25; Mentions in annual reports (R) = 0.15; Website search results (W) = 0.15. Introducing these weights ensures that a DPA's activity in issuing decisions has a greater impact on the score than mentions of AI in reports or websites. As decisions are legally binding, they should carry more weight in assessing DPAs' activities. However, we must also consider that identifying the relevant decisions poses the most

GDPR's provisions and national blacklists. Our results prove that this is the case, for example, in the opinion adopted by the Bulgarian DPA — see Section IV.

significant technical challenge when collecting data for analysis (e.g., due to limitations in website search functions or DPAs not publishing their choices). Therefore, we concluded that the indicator's overall decision weight — understood as the joint weight of AI-related and ADM-specific decisions — should be set to 0.5. Next, the DPIA blacklist inclusion indicator was assigned a weighted value of 0.2, while the soft, non-legally binding indicators — Mentions in annual reports and Website search results — together have a weighted value of 0.3. The index is calculated using the following formula:

$$I = 0.20 \cdot B + 0.25 \cdot D_{AI} + 0.25 \cdot D_{ADM} + 0.15 \cdot R + 0.15 \cdot W$$

The index may have a value between 0 and 1.

Table 3 shows the values of all indicators and the index calculated using this formula. The higher the index's value, the greater the DPA's activity level concerning enforcing AI-driven products and services and the provisions that may be important for enforcing the *AI Act*. For the Member States in which enforcement is divided between the national and regional levels (Germany and Spain, marked with italics in Table 3), values relating to results, reports, and blacklists are based on the national level (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* — BfDI and *Agencia Española de Protección de Datos* — AEPD). Regarding decisions, we focused on the AEPD in Spain. In Germany, our search and literature review identified multiple choices in both the AI and ADM categories. Therefore, we applied a score of 1 to both of these categories.

MS \ Indicator	DPIA blacklist inclusion	AI-related decisions	ADM-specific decisions	Mentions in annual reports	Website search results	INDEX: VALUE
Austria	1	1	1	0,75	0,5	0,89
Belgium	0,5	0,5	1	0,75	0,75	0,70
Bulgaria	0,5	0,5	1	0,75	0,75	0,70
Croatia	0,5	0	0	0,75	0,75	0,33
Cyprus	0,5	0	0,5	0	0,25	0,26
Czech Republic	0,5	0,5	0,5	0,75	0,5	0,54
Denmark	0,75	1	0,5	0,75	1	0,79
Estonia	0,5	0	0	1	0,5	0,33
Finland	0,5	0,5	1	0,75	0,75	0,70
France	0,5	1	1	1	1	0,90
Germany	1	1	1	1	1	1,00
Greece	1	0,5	1	0,75	1	0,84
Hungary	0,5	0,5	0,5	0,75	0,5	0,54
Ireland	0,5	0,5	0	0,5	1	0,45

Italy	1	1	1	0,75	1	0,96
Latvia	0,5	0,5	1	0,5	0,75	0,66
Lithuania	0,5	0	0,5	0,75	0,25	0,38
Luxembourg	0,75	0,5	1	0,75	0,75	0,75
Malta	0,5	0	0	0,75	0,25	0,25
Netherlands	0,5	1	1	1	1	0,90
Poland	0,75	0	0	0,75	0,75	0,38
Portugal	0,5	1	1	0,75	0,5	0,79
Romania	0,5	0	0,5	0,5	0	0,30
Slovakia	0,5	0	0	0,5	0,25	0,21
Slovenia	0,5	0,5	1	0,75	0,75	0,70
Spain	0,75	1	1	1	1	0,95
Sweden	0,5	0,5	1	1	0,75	0,74

Table 3: The values of all the indicators and the index.

While our index captures the volume of AI-related enforcement, a complete picture of regulatory effectiveness also requires substantial qualitative evidence. Subsequent studies should, therefore, examine the endurance of decisions (are DPAs' decisions frequently overturned or remitted on appeal during judicial review?), the argumentative robustness of decisions (how thoroughly do they engage with technical facts, risk assessments, and proportionality analysis?), and perceptions of legitimacy (how do experts, regulated entities, and civil society stakeholders rate the clarity, fairness, and practical impact of DPAs' reasoning?). We did not address these dimensions in this study because the qualitative coding of legal reasoning is politically sensitive and time-consuming. This would slow down the assessment process relative to the pace at which *AI Act* oversight must now scale. One pragmatic solution would be to re-audit DPAs on a rolling basis — for example, every two or three years — using qualitative indicators. The EU-wide decision database we propose in Section V would provide the basis for such peer review and, in turn, provide targeted capacity building or guidance to authorities whose reasoning or success rates are suboptimal. In short, the quantitative index provides the rapid approach that *AI Act* enforcement now requires. At the same time, a structured, periodic qualitative audit could deliver the fine-tuning demanded by long-term, high-quality enforcement.

IV. HOW ACTIVE ARE THE DPAS IN THE ENFORCEMENT RELATED TO AI?

The final step of our empirical analysis is to group the Member States according to their activity level in enforcing AI-related matters. The Member States are divided into four groups. The first group comprises very active enforcers (score: 0.85–1.00, marked dark green in Table 3). The second group includes active enforcers (score: below 0.85–0.60, marked light green). The third group comprises reluctant enforcers (score: below 0.6–0.40–0.59, marked yellow). The fourth group includes inert enforcers (score: below 0.40, marked red). This section elaborates on the characteristics of each group, providing examples of enforcement activities undertaken by Member States belonging to each group to illustrate the DPAs' levels of activity through concrete decisions and other undertakings.

Very Active Enforcers

The first group we identified comprises the very active enforcers: Austria, France, Germany, Italy, the Netherlands, and Spain. In the case of all these countries, we identified more than one decision or opinion in the categories of 'AI-related decisions' and 'ADM-specific decisions' in the case of all these countries. Each of these DPAs also undertakes other categories of activity considered in our study, resulting in numerous findings on the website and the DPAs' annual reports. The issue of blacklists is the most varied, with the DPAs in this group taking different approaches.

To illustrate the characteristics of this group, we have selected Italy and Spain as examples. Italy is notable for its active approach to companies providing AI tools. Compared to most DPAs, the Italian authority, the *Garante per la Protezione dei Dati Personali* (Garante), is known for promptly commencing proceedings regarding the compliance of new technological tools with data protection regulations. The decisions concerning OpenAI's ChatGPT[31] and DeepSeek[32] are the best examples of this approach. While other DPAs limited their actions to issuing guidelines on using Large Language Models (LLMs), the Garante temporarily blocked these tools. The Garante is also one of the DPAs whose investigation into Clearview AI's activities resulted in a fine of 20 million euros.[33]

In addition to these proceedings, the Garante is also very active in the other categories examined in our study. Firstly, Italy is one of the few countries where AI is mentioned directly on the blacklist. Furthermore, the numerous mentions of AI in annual reports from 2021 to 2023, along with the multiple findings on the website — including a dedicated subpage on AI[34] — demonstrate the Italian DPA's keen interest in AI-driven services, as well as the implications and risks posed by their use to personal data protection. These indicators collectively reflect Garante's active approach to enforcement.

The Spanish DPA (AEPD) is also one of the most active enforcers in the area of AI. We identified several decisions relating to AI and ADM to some extent. However, it is worth noting that the Spanish DPA is less active than the Garante in adopting AI-related decisions. In the investigations initiated by the AEPD, the AI element was mostly ancillary, meaning the proceedings were not directed at companies focusing on AI or ADM per se. Instead, the AI element was considered one of many aspects of the case. For instance, regarding ADM, the Spanish DPA fined CaixaBank 3 million euros for profiling for marketing purposes without obtaining valid consent, as it was neither specific nor informed.[35]

It should be noted that, in 2020, the AEPD also issued guidelines on the intersection of the GDPR and AI: *GDPR compliance of processing that embeds Artificial Intelligence. An introduction*.[36] These guidelines provide a practical overview of how to ensure that products and services using AI comply with the GDPR. The focus is on transparency, the legal basis for processing, data subject rights, ADM, and DPIAs. Furthermore, the Spanish DPA's active approach to enforcing AI is evident from the numerous mentions of AI (approximately 200) on its website and in its annual reports from 2021 to 2023. These include sources concerning various events, educational materials, and information on AI's challenges to data protection.

Active Enforcers

The largest cohort consists of DPAs for which we identified at least one formal decision or opinion in both the 'AI-related decisions' and 'ADM-specific decisions' categories, or at least one in one category and multiple

[31] See Garante, 'Decision 9870832' (30 March 2023) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832> accessed 28 April 2025.
[32] See Garante, 'Decision 10098477' (30 January 2025) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10098477> accessed 28 April 2025.
[33] See Garante, 'Decision 9751362' (10 February 2022) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362> accessed 28 April 2025.
[34] Garante's subpage dedicated solely to AI, see <https://www.garanteprivacy.it/temi/intelligenza-artificiale> accessed 28 April 2025.
[35] See AEPD, 'Decision PS/00500/2020' (21 October 2021) <https://www.aepd.es/documento/ps-00500-2020.pdf> accessed 28 April 2025.
[36] See AEPD, 'Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción' (13 February 2020) <https://www.aepd.es/media/guias/adecuacion-rgpd-ia.pdf> accessed 28 April 2025.

in the other. These countries also achieved moderate-to-high scores on other indicators in our study. This group includes countries from across the EU, encompassing both 'old' and 'new' Member States, such as Belgium, Bulgaria, Denmark, Finland, Greece, Latvia, Luxembourg, Portugal, Slovenia, and Sweden.

To illustrate the types of DPAs that belong to this group, we selected Greece and Bulgaria as examples. In Greece, decisions relating to AI include proceedings concerning a complaint against Clearview AI,[37] and a decision regarding the company Cosmote concerning the processing of biometric data.[38] Regarding ADM, we identified one decision in which an infringement was found concerning the use of Centaur and Superion programs by the Ministry of Migration and Asylum,[39] as well as one decision in which an infringement concerning ADM use was considered but not found.[40] Greece also undertook an *ex officio* investigation of DeepSeek's data processing activities.[41] It is also one of the countries that explicitly mentions AI in its list of types of processing requiring a DPIA.[42] These factors demonstrate a certain level of experience with enforcing AI-based services and an active approach to addressing this issue.

The presence of the 'new' Member States, Bulgaria and Slovenia, in this category is worth highlighting. Regarding Bulgaria, we found an opinion about using facial recognition technology in schools. The DPA stated that such a solution would contravene the GDPR.[43] We also identified an opinion on regulating the National Health Information System. This opinion, which was issued in response to a request for consultation on DPIA, raised the issue of potential non-compliance with the *AI Act*.[44] We also identified an opinion on using biometric data to control access to sports centres by technical means.[45] This opinion was also issued in response to the DPIA consultation request and stated that such a system would infringe Article 22 of the GDPR.[46] Regarding the soft indicators, the Bulgarian DPA has, e.g., educational materials on AI, as well as information on how to object to Meta's processing of personal data for AI training purposes, on its website.[47]

---

[37] See Hellenic Data Protection Authority (HDPA), 'Decision 35/2022' (13 July 2022) <https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf> accessed 28 April 2025.

[38] See HDPA, 'Decision 57/2022' (26 October 2022) <https://www.dpa.gr/sites/default/files/2023-01/57_2022%20anonym.pdf> accessed 28 April 2025.

[39] See HDPA, 'Decision 13/2024' (2 April 2024) <https://www.dpa.gr/sites/default/files/2024-04/13_2024%20anonym.pdf> accessed 28 April 2025.

[40] See HDPA, 'Decision 51/2021' (19 November 2022) <https://www.dpa.gr/sites/default/files/2021-12/51_2021anonym.pdf> accessed 28 April 2025.

[41] See HDPA, 'The Authority's investigations for the TN application and for malicious software' [Έρευνες της Αρχής για εφαρμογή TN και για κακόβουλο λογισμικό] (6 February 2022) <https://www.dpa.gr/el/enimerwtiko/deltia/ereynes-tis-arhis-gia-efarmogi-tn-kai-gia-kakoboylo-logismiko> accessed 28 April 2025.

[42] See HDPA, 'Decision 65/2018' (16 October 2018) <https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf> accessed 28 April 2025.

[43] See Commission for Personal Data Protection (CPDP), 'Opinion of the CPDP regarding the installation of facial recognition entry-exit cameras connected to a school's electronic diary' [Становище на КЗЛД относно монтиране на входно-изходни камери за лицево разпознаване, свързани с електронен дневник на училище] (21 December 2018) <https://cpdp.bg/становище-на-кзлд-относно-монтиране-н-2/> accessed 28 April 2025.

[44] See CPDP, 'Opinion [...] regarding: A request for prior consultation under Article 36, paragraph 4 of Regulation (EU) 2016/679 has been received in connection with the development of a draft Regulation on the functioning of the National Health Information System' [СТАНОВИЩЕ [...] ОТНОСНО: Постъпило искане за предварителна консултация по чл. 36, пар. 4 от Регламент (ЕС) 2016/679 във връзка с изработването на проект на Наредба за функционирането на Националната здравноинформационна система.] (14 September 2022) <https://cpdp.bg/wp-content/uploads/2023/08/Stanovishte_KZLD-Naredba_NZIS_14.09.2022.pdf> accessed 28 April 2025.

[45] Due to the word count constraints, we do not provide here more examples, but they may be found in Mazur, Novelli and Choińska (n 21).

[46] See CPDP, 'CPDP Opinion on the use of biometric data for control by technical means of access to sports centres' [Становище на КЗЛД относно използването на биометрични данни за контрол чрез технически средства за достъп до спортни центрове] (29 April 2024) <https://cpdp.bg/искане-за-предварителна-консултация/?hilite=Автоматизирано+вземане+индивидуални+решения#_ftnref3> accessed 28 April 2025.

[47] See CPDP, 'Information about data subjects about Meta's intent to use photos and publications of users of social networks to train its artificial intelligence' [Информация за субектите на данни относно намерението на Meta да използва снимки и публикации на потребителите на социалните ѝ мрежи, за да обучава изкуствения си интелект] (12 June 2024) <https://cpdp.bg/информация-за-субектите-на-данни-отно/?hilite=изкуствения+интелект> accessed 28 April 2025.

Reluctant Enforcers

The smallest group comprises the Czech Republic, Hungary, and Ireland, which we have classified as 'reluctant enforcers.' In any of the scrutinised categories (either AI-related or ADM-specific), we identified no more than one decision in any of these jurisdictions. In Ireland, we only identified initiated proceedings, not adopted decisions. The Czech Republic and Hungary exhibit characteristics indicating moderate activity, as indicated by the number of results identified on their websites. However, Ireland seems to be more active in terms of the assessment based on this indicator. It should be noted, though, that the website's search engine provides numerous — but not necessarily precise — results.

A specific case in Hungary involved potential infringements of several provisions, including Article 22 of the GDPR and the use of AI.[48] The proceedings were initiated *ex officio* and related to the bank's processing of data from recordings of conversations with customers. Contrary to the bank's claims, the DPA ruled that the solutions employed 'belong to the realm of artificial intelligence.'[49] The DPA found numerous infringements of GDPR provisions in this case, even though not of Article 22, and imposed a fine.

Although several major tech companies that provide AI solutions are registered in Ireland, the Irish *Data Protection Commission* (DPC) is not particularly active in enforcing AI legislation. We could not identify any decisions concerning AI or Article 22 of the GDPR that had been adopted. Nevertheless, two recent investigations have been initiated regarding the training of LLMs: Google AI Model[50] and Grok[51] (an LLM provided by X). The annual reports of the Irish DPA also demonstrate a reluctance to exercise enforcement activities concerning AI. Between 2021 and 2023, AI was either not mentioned at all or only mentioned once in a vague manner.

These results were unsurprising, given the DPC's well-known reluctance to issue fines or initiate investigations against major technology companies. Furthermore, Ireland has recently been criticised for introducing an amendment to the Irish Data Protection Act that enables the DPC to classify its documents as 'confidential,'[52] thereby reducing the transparency of its proceedings. This reluctant approach to enforcement has resulted in several of the DPC's decisions being overruled by the EDPB—a precedent that had not previously been established for any other European DPA.[53] However, there are hardly any signs that the DPC is changing its approach.

Inert Enforcers

The group of inert enforcers comprises eight countries, all of which are 'new' Member States. For most of these countries, namely Croatia, Estonia, Malta, Poland,[54] and Slovakia, we could not identify any decisions concerning AI or ADM. In the case of Cyprus, Lithuania, and Romania, we identified one decision relating to ADM. However, poor results on other indicators gave these countries a similar overall score to those in this

[48] See Hungarian National Authority for Data Protection and Freedom of Information (NAIH) 'Decision NAIH-85/2022 (NAIH-7350/2021)' (8 February 2022) <https://www.naih.hu/data-protection/decisions?download=522:ai-based-speech-signal-processing-technology-and-data-protection> accessed 28 April 2025 [English version].
[49] See ibid, para. 68.
[50] DPC, 'Data Protection Commission launches inquiry into Google AI model' (12 September 2024) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-launches-inquiry-google-ai-model#AI> accessed 28 April 2025.
[51] DPC, 'Data Protection Commission Announces commencement of inquiry into X Internet Unlimited Company (XIUC)' (11 April 2025) <https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-announces-commencement-inquiry-x-internet-unlimited-company-xiuc#artificial%20intelligence> accessed 28 April 2025.
[52] See noyb, 'Ireland makes questionable GDPR cases 'confidential'. Irish DPC will likely use Section 26A to muzzle criticism' (29 June 2023) <https://noyb.eu/en/ireland-corrupt-gdpr-procedures-now-confidential> accessed 28 April 2025.
[53] See European Data News Hub — Agence France-Presse, 'How Ireland became the EU's reluctant data privacy enforcer' (23 May 2023) <https://ednh.news/en/how-ireland-became-eus-reluctant-data-privacy-enforcer/> accessed 28 April 2025.
[54] In the case of Poland, there are ongoing proceedings concerning OpenAI. However, no decision had been adopted at the time of data collection, see Anna Wittenberg, 'Ta decyzja może wywrócić model biznesowy OpenAI. Prezes UODO: zapadnie do końca roku' (30 May 2025, WNP.PL) <https://www.wnp.pl/tech/ta-decyzja-moze-wywrocic-model-biznesowy-openai-prezes-uodo-zapadnie-do-konca-roku,949376.html> accessed 30 May 2025.

group. Despite the low scores relating to the identified decisions, it should be noted that these DPAs have published information on various AI-related activities on their websites and in their annual reports (e.g., participation in supranational initiatives and events on this topic).

It is problematic to assess the activity level of some of the inert enforcers regarding AI due to the poor quality of the DPAs' websites. Romania is an example of this: its low result is also linked to its website's lack of a search function. Nevertheless, even DPAs with higher-quality websites can be inactive in this area (e.g., Cyprus and Malta). Of the inert enforcers, Lithuania and Poland achieved the highest scores. In Lithuania's case, this is linked to identifying a decision relating to ADM. Poland's score was achieved despite the absence of any decisions concerning ADM or AI. However, we observed the DPA participating in other activities.

V. THE POTENTIAL INVOLVEMENT OF THE DPAS IN THE ENFORCEMENT OF THE *AI ACT*

Our findings show that, while all DPAs are active in AI-related enforcement to some extent, there are significant differences in their level of experience. In this section, we use our results to answer the question of how DPAs should be involved in enforcing the *AI Act*, given their activity level in AI-related enforcement. As explained in Section II, the *AI Act* directly obliges Member States to designate DPAs as MSAs in certain situations or otherwise addresses the need to include DPAs in enforcing the *AI Act* (e.g., in the case of AI regulatory sandboxes). Therefore, our suggestions concern the involvement of DPAs, which is not obligatory under the *AI Act*'s provisions.

We argue that DPAs should be involved in enforcing Article 86 of the *AI Act* — the right to an explanation of individual decision-making. The empirical results of our study and the fact that at least 21 DPAs have experience enforcing ADM strongly support the designation of DPAs as responsible for handling proceedings related to this article. This would enable the enforcer to leverage the expertise that many DPAs have gathered to date for the purpose of enforcing the *AI Act*. From a strictly legal perspective, this solution is also supported by its similarity to Articles 13(2)(f), 14(2)(g), and 15(1)(h) in relation to Article 22 of the GDPR. Furthermore, it guarantees the right to an explanation of ADM 'only to the extent that the right [...] is not otherwise provided for under Union law.'[55] Therefore, to coordinate enforcement, it would be sensible to assign powers relating to this provision to the DPAs.

Next, our analysis supports the inclusion of DPAs as a category of MSAs. Their competencies extend beyond those outlined in Article 74 of the *AI Act*, making them well-suited to overseeing key high-risk areas. Specifically, we recommend involving DPAs in the monitoring of AI systems used in education and vocational training, employment, management of workers, access to self-employment, and access to and enjoyment of essential private and public services and benefits (points 3, 4, and 5 of Annex III of the *AI Act*). As these areas frequently involve ADM based on personal data, the expertise[56] of DPAs is highly relevant to effective enforcement.

From an empirical perspective, the results of our study indicate that over two-thirds (19) of the DPAs have experience with enforcement in cases involving AI-based services. This finding lends weight to the suggestion that they should be designated as MSAs under the AI Act. Furthermore, as AI tools involving personal data processing become more widespread, it is reasonable to expect an increase in the number of proceedings initiated and decisions issued by DPAs regarding AI-driven solutions, particularly given that existing cases demonstrate the interest of many DPAs in this issue.

However, our analysis also shows that DPAs' experience varies significantly. We identified more than one DPA decision concerning AI in only eight Member States. Considering the varying levels of DPA activity regarding AI and ADM legislation enforcement, we recognise the risks associated with designating reluctant and inert enforcers as MSAs. While active DPAs could benefit from stronger investigatory powers under the *AI Act* (see Section II), assigning these powers to reluctant enforcers raises concerns about underenforcement, potentially leading to inconsistent implementation of the *AI Act* across the EU. On the other hand, an

[55] *AI Act*, Art 86(1).

[56] For example, *AI Act*, Annex III, point 3 lett. d refers to 'AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.' Latvian DPA issued a decision concerning this type of system, see Datu valst inspekcija, 'Lēmums Nr.2-2.2/17' (1 July 2020) <https://www.dvi.gov.lv/lv/media/899/download?attachment> accessed 29 May 2025.

enforcement system based on national institutions will always entail differences in the activity level between Member States. Reluctant and inert enforcement may result from organisational aspects of the authorities' functioning, e.g., a lack of financial and human resources or necessary expertise.[57] While scrutinising these issues exceeds the scope of our study, it should be noted that such problems may often affect more than one enforcement agency in a given Member State.[58] Therefore, this may be considered a systemic problem concerning the enforcement of EU law. In light of this, decisions concerning designation at the level of Member States may not be that vital for the activity level represented by the enforcer.

Despite the systemic nature of the challenges related to enforcement, some measures can facilitate enforcement by less active authorities. One way to reduce discrepancies in activity levels among enforcers in different Member States is to strengthen the position of supranational bodies within the enforcement system. Although enforcement is predominantly assigned to national institutions under both EU data protection law and the *AI Act*, bodies and networks operating at the EU level also play a role. The materials we examined during the study confirm that, in the case of DPAs, the existing body — the EDPB — is used to share knowledge and expertise.[59] The materials analysed for our study demonstrate the importance of the EDPB for many DPAs, as the EDPB's statements and documents are frequently referenced in some DPAs' annual reports.[60] Furthermore, cooperation between DPAs seems to encourage the authorities to share solutions to common problems or challenges. For instance, the Latvian DPA (an active enforcer) posted a link on its website to the Spanish DPA's (a very active enforcer) tool for DPIA,[61] and the Hungarian DPA (a reluctant enforcer) posted a link to the French DPA's tool (a very active enforcer).[62]

We argue that the existence of such a well-established network is an essential factor to consider when designing the enforcement system for the *AI Act* and ensuring consistency between Member States. What deserves further attention, therefore, is the interplay between the activities of the EDPB and the AI Board, the core members of which include one representative from each Member State.[63] The *AI Act* allows the EDPS to be included as an observer in the AI Board structure.[64] Other authorities may be invited to AI Board meetings on a 'case-by-case basis, where the issues discussed are of relevance to them.'[65] Given the activity level of many DPAs and the

---

[57] The Lithuanian DPA, for example, mentions this issue directly in its annual report, emphasising its importance for the enforcement of AI: 'In the future, the difficulties in attracting new employees may increase due to changes in legal regulation (data management, use of artificial intelligence, etc.), as well as due to the fact that there are differences in the salary offered in the public and private sectors on the labour market. In addition to the aforementioned unfavourable factors, the Inspectorate is also faced with difficulties in finding employees with specific competencies (personal data protection, data security or cybersecurity, auditing, data management, etc.).' — Valstybinė Duomenų Apsaugos Inspekcija, '2024. M. Veiklos Ataskaita' (2025) 17, <https://vdai.lrv.lt/public/canonical/1740980215/759/2024_m._VDAI_veiklos_ataskaita_2025_02_28_4R-104%20(1.7%20E).pdf>, accessed 30 May 2025 [automated translation using Google Translate]. For the discussion of this issue on the basis of empirical research, see also European Union Agency for Fundamental Rights (FRA), 'GDPR in practice – Experiences of data protection authorities' (11 June 2024) 59–63, <https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities>, accessed 30 May 2025.

[58] Therefore, it may not be beneficial to include other authorities operating in the given Member State alongside the DPAs as MSAs, as designating multiple authorities as MSAs could lead to the enforcement process becoming fragmented. However, coordination between the various enforcers at Member State level is advisable, see FRA, ibid, 63, which indicates 'DPAs coordinating the supervision of AI with other national regulators' as a promising practice.

[59] For example, see the Support Pool of Experts (SPE), implemented under the EDPB's 2024–2027 strategy. This initiative's projects aim to help DPAs enhance their enforcement capabilities in areas such as AI and data protection, providing them with access to a diverse pool of experts in these fields: EDPB, 'EDPB publishes final version of guidelines on data transfers to third country authorities and SPE training material on AI and data protection' (5 June 2025) <https://www.edpb.europa.eu/news/news/2025/edpb-publishes-final-version-guidelines-data-transfers-third-country-authorities-and_en> accessed 9 June 2025.

[60] For example, five out of seven mentions of AI in the 2022 report of the Croatian DPA concern activities undertaken within the EDPB framework, see Godišnje Izvješće Agencije Za Zaštitu Osobnih Podataka, 'Godišnje izvješće o radu 2022' (2023) 82, <https://azp.hr/wp-content/uploads/2023/12/AZOP_Izvjesce-2022.pdf> accessed 6 June 2025.

[61] See Datu valst inspekcija, 'Rīks datu apstrādes reģistra un risku analīzei' (13 July 2023) <https://www.dvi.gov.lv/lv/riks-datu-apstrades-registra-un-risku-analizei> accessed 29 May 2025.

[62] See NAIH, 'Adatvédelmi hatásvizsgálati szoftver' <https://www.naih.hu/hatasvizsgalati-szoftver> accessed 6 June 2025.

[63] See Art 65(2), *AI Act.*

[64] See Art 65(2), *AI Act.*

[65] Art 65(2), *AI Act.*

importance of the EDPB for AI-related cooperation, we advocate using this possibility, particularly when dealing with high-risk AI systems.

From a legal analysis perspective, the case for designating DPAs as MSAs may be strengthened by observing that DPAs should be consulted by the data controller regarding the performance of a DPIA in cases involving high-risk AI systems that process personal data. Article 36(1) of the GDPR states the following: 'The controller shall consult the supervisory authority before processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.' This wording could mean that high-risk AI systems under the *AI Act* fulfil this condition, as such systems are literally defined as high-risk. Therefore, aligning the GDPR and *AI Act* enforcement in this regard could be beneficial.

Our final suggestion relates to the practical aspects of enforcement based on our observations when conducting the study. Decentralised enforcement of EU data protection law presents several challenges, one of which is identifying similar cases in other Member States. While technological tools, particularly automated translation, facilitate the search for decisions issued by various DPAs, challenges concerning access to these decisions cannot be resolved without greater coordination and transparency from the relevant authorities. Furthermore, any more detailed analysis of the decision-making practices of the enforcement bodies is complex due to the limitations of the available sources. We lack comprehensive information about the decisions issued by the DPAs, judicial reviews of these decisions, the imposed sanctions, and other consequences of the proceedings. Given the EU-wide reach of many of the services and products in question, it is advisable to adopt common standards for publishing decisions and establish a common database to enable citizens to access the decisions of various DPAs. This suggestion is relevant regardless of Member States' choices concerning enforcing the *AI Act*, as it would facilitate enforcement by increasing transparency regarding cases involving AI-driven services and products across the EU.

IV. CONCLUSIONS

Our study begins with analysing the DPAs' position under the *AI Act*, noting that this regulation leaves much discretion regarding the role the DPAs may play in its enforcement system. Next, we present a unique dataset collecting data on five indicators relating to enforcing data protection law in relation to AI-driven services and products. Using this dataset, we examine the activity level exhibited by the DPAs regarding the enforcement related to AI.

We propose a weighted index based on which Member States are divided into four groups. The first group comprises the very active enforcers: Austria, France, Germany, Italy, the Netherlands, and Spain. These DPAs issued more than one decision or opinion in categories concerning AI-related and ADM-specific choices, as well as exhibited activity in other categories. The second group comprises active enforcers (Belgium, Bulgaria, Denmark, Finland, Greece, Latvia, Luxembourg, Portugal, Slovenia, and Sweden). These are the DPAs that we identified as having issued at least one decision or opinion in the AI-related and ADM-specific categories (or one in one category and multiple in the other), as well as having moderate-to-high scores in different indicators. The third group comprises the reluctant enforcers: the Czech Republic, Hungary, and Ireland. We could not identify more than one decision in any of the examined categories for these Member States. Fourthly, the inert enforcers: We could not identify any AI-related or ADM-specific decisions in the case of Croatia, Estonia, Malta, Poland, and Slovakia. In the case of Cyprus, Lithuania, and Romania, we identified one ADM-related decision. However, their low scores on other indicators resulted in an overall score similar to that of the other inert enforcers.

Based on these results, we propose two solutions regarding the involvement of DPAs in enforcing the *AI Act*. Firstly, given that many DPAs already have experience enforcing provisions governing ADM, we suggest designating them as the authorities responsible for handling complaints under Article 86 of the *AI Act*. This article provides the right to an explanation regarding the use of AI systems for high-risk purposes. Secondly, given the level of DPA activity regarding AI-related enforcement, we advocate designating DPAs as MSAs. The DPAs should be responsible for enforcing the provisions concerning high-risk AI systems listed in Annex III, points 3–5, of the *AI Act*. The possible intersections between the MSAs' enforcement of some high-risk uses under the *AI Act* and the enforcement of such solutions resulting from data protection law (e.g., DPIA consultations) further support our suggestion. We advocate strengthening supranational cooperation among

enforcers to mitigate the risks associated with designating reluctant and inert DPAs as MSAs. Lastly, we propose creating an EU-wide database to collect decisions issued by DPAs. This would significantly improve transparency in the decentralised enforcement model adopted under the GDPR and, to a large extent, the *AI Act*.

V. REFERENCES

Bachňáková Rózenfeldová Laura et al., 'Personal Data Protection Enforcement under GDPR — the Slovak Experience' (2024) 14(3) *International Data Privacy Law* 278.

Brkan Maja, '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

Digibeetle, 'List of authorities protecting fundamental rights (Article 77 AI Act)' (12 March 2025) <https://www.linkedin.com/posts/jbagerritsen_digibeetles-list-of-art-77-ai-act-authorities-activity-7305605824750493708-A5Oq?utm_source=share&utm_medium=member_desktop&rcm=ACoAACDTwaQBHkcKWW9-dGRe5PzeeYkZA-DbjaI> accessed 19 May 2025.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), OJ 2016 L119/89.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (ePrivacy directive), OJ 2002 L 201/37.

EDPB, 'EDPB publishes final version of guidelines on data transfers to third country authorities and SPE training material on AI and data protection' (5 June 2025) <https://www.edpb.europa.eu/news/news/2025/edpb-publishes-final-version-guidelines-data-transfers-third-country-authorities-and_en> accessed 9 June 2025.

EDPB, *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework* (Statement 3/2024) (16 July 2024) <https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf> accessed 9 June 2025.

European Data News Hub — Agence France-Presse, 'How Ireland became the EU's reluctant data privacy enforcer' (23 May 2023) <https://ednh.news/en/how-ireland-became-eus-reluctant-data-privacy-enforcer/> accessed 28 April 2025.

European Union Agency for Fundamental Rights (FRA), 'GDPR in practice – Experiences of data protection authorities' (11 June 2024) 59–63, <https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities>, accessed 30 May 2025.

Kaminski Margot E and Gianclaudio Malgieri, 'The Right to Explanation in the AI Act' (2025) *U of Colorado Law Legal Studies Research Paper No. 25-9*, <https://ssrn.com/abstract=5194301> accessed 31 May 2025.

Kaminski Margot E, 'The Right to Explanation, Explained' (2019) 34 *Berkeley Technology Law Journal* 189.

Malgieri Gianclaudio and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7(4) *International Data Privacy Law* 243

Malgieri Gianclaudio, 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations' (2019) 35(5) *Computer Law & Security Review* 105327

Mazur Joanna and Zuzanna Choińska, 'European Union data protection law and the use of facial recognition technology for the purpose of fighting crime,' in Michał Balcerzak and Julia Kapelańska-Pręgowska (eds), *Artificial Intelligence and International Human Rights Law* (Edward Elgar Publishing 2024) 124–144.

Mazur Joanna, 'Artificial Intelligence vs Data Protection: How the GDPR Can Help to Develop a Precautionary Regulatory Approach to AI?', in Angelos Kornilakis, Georgios Nouskalis, Vassilis Pergantis and Themistoklis Tzimas (eds) *Artificial Intelligence and Normative Challenges (Law, Governance and Technology Series, vol 59)* (Springer 2023) 215–223.

Metikoš Ljubiša and Jef Ausloos, 'The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act' (2025) 17(1) *Law, Innovation and Technology* 205.

Novelli Claudio, Philipp Hacker, Jessica Morley, Jarle Trondal and Luciano Floridi, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) *European Journal of Risk Regulation* 1, https://doi.org/10.1017/err.2024.57.

noyb, 'Ireland makes questionable GDPR cases 'confidential'. Irish DPC will likely use Section 26A to muzzle criticism' (29 June 2023) <https://noyb.eu/en/ireland-corrupt-gdpr-procedures-now-confidential> accessed 28 April 2025.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ 2024 L 1689.

Ruohonen Jukka and Kalle Hjerppe, 'The GDPR enforcement fines at a glance' (2022) 106 *Information Systems* 101876

Puljak Livia, Anamaria Mladinić and Zvonimir Koporc, 'Workload and procedures used by European data protection authorities related to personal data protection: a cross-sectional study' (2023) 16(41) *BMC Res Notes* 1

Selbst Andrew D and Julia Powles, 'Meaningful information and the right to explanation' (2017) 7(4) *International Data Privacy Law* 233

Sivan-Sevilla Ido, 'Varieties of Enforcement Strategies Post-GDPR: A Fuzzy-Set Qualitative Comparative Analysis (fsQCA) across Data Protection Authorities' (2022) 31(2) *Journal of European Public Policy* 552

Sun Chen et al., 'GDPRxiv: Establishing the State of the Art in GDPR Enforcement' (2023) 4 *Proceedings on Privacy Enhancing Technologies* 484.

Wachter Sandra, Brendt Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76

Wittenberg Anna, 'Ta decyzja może wywrócić model biznesowy OpenAI. Prezes UODO: zapadnie do końca roku' (30 May 2025, WNP.PL) <https://www.wnp.pl/tech/ta-decyzja-moze-wywrocic-model-biznesowy-openai-prezes-uodo-zapadnie-do-konca-roku,949376.html> accessed 30 May 2025.

National decisions, information on proceedings, and other documents

AEPD, 'Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción' (13 February 2020) <https://www.aepd.es/media/guias/adecuacion-rgpd-ia.pdf> accessed 28 April 2025.

AEPD, 'Decision PS/00500/2020' (21 October 2021) <https://www.aepd.es/documento/ps-00500-2020.pdf> accessed 28 April 2025.

CPDP, 'CPDP Opinion on the use of biometric data for control by technical means of access to sports centres' [Становище на КЗЛД относно използването на биометрични данни за контрол чрез технически средства за достъп до спортни центрове] (29 April 2024) <https://cpdp.bg/искане-за-предварителна-консултация/?hilite=Автоматизирано+вземане+индивидуални+решения#_ftnref3> accessed 28 April 2025.

CPDP, 'Information about data subjects about Meta's intent to use photos and publications of users of social networks to train its artificial intelligence' [Информация за субектите на данни относно намерението на Meta да използва снимки и публикации на потребителите на социалните ѝ мрежи, за да обучава изкуствения си интелект] (12 June 2024) <https://cpdp.bg/информация-за-субектите-на-данни-отно/?hilite=изкуствения+интелект> accessed 28 April 2025.

CPDP, 'Opinion [...] regarding: A request for prior consultation under Article 36, paragraph 4 of Regulation (EU) 2016/679 has been received in connection with the development of a draft Regulation on the functioning of the National Health Information System' [СТАНОВИЩЕ [...] ОТНОСНО: Постъпило искане за предварителна консултация по чл. 36, пар. 4 от Регламент (ЕС) 2016/679 във връзка с изработването на проект на Наредба за функционирането на Националната здравноинформационна система.] (14 September 2022) <https://cpdp.bg/wp-content/uploads/2023/08/Stanovishte_KZLD-Naredba_NZIS_14.09.2022.pdf> accessed 28 April 2025.

CPDP, 'Opinion of the CPDP regarding the installation of facial recognition entry-exit cameras connected to a school's electronic diary' [Становище на КЗЛД относно монтиране на входно-изходни камери за лицево разпознаване, свързани с електронен дневник на училище] (21 December 2018) <https://cpdp.bg/становище-на-кзлд-относно-монтиране-н-2/> accessed 28 April 2025.

Datu valst inspekcija, 'Lēmums Nr.2-2.2/17' (1 July 2020) <https://www.dvi.gov.lv/lv/media/899/download?attachment> accessed 29 May 2025.

Datu valst inspekcija, 'Rīks datu apstrādes reģistra un risku analīzei' (13 July 2023) <https://www.dvi.gov.lv/lv/riks-datu-apstrades-registra-un-risku-analizei> accessed 29 May 2025.

DPC, 'Data Protection Commission Announces commencement of inquiry into X Internet Unlimited Company (XIUC)' (11 April 2025) <https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-announces-commencement-inquiry-x-internet-unlimited-company-xiuc#artificial%20intelligence> accessed 28 April 2025.

DPC, 'Data Protection Commission launches inquiry into Google AI model' (12 September 2024) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-launches-inquiry-google-ai-model#AI> accessed 28 April 2025.

Garante, 'Decision 10098477' (30 January 2025) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10098477> accessed 28 April 2025.

Garante, 'Decision 9751362' (10 February 2022) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362> accessed 28 April 2025.

Garante, 'Decision 9870832' (30 March 2023) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832> accessed 28 April 2025.

Garante, Garante's subpage dedicated solely to AI, see <https://www.garanteprivacy.it/temi/intelligenza-artificiale> accessed 28 April 2025.

Godišnje Izvješće Agencije Za Zaštitu Osobnih Podataka, 'Godišnje izvješće o radu 2022' (2023) 82, <https://azp.hr/wp-content/uploads/2023/12/AZOP_Izvjesce-2022.pdf> accessed 6 June 2025.
HDPA, 'Decision 13/2024' (2 April 2024) <https://www.dpa.gr/sites/default/files/2024-04/13_2024%20anonym.pdf> accessed 28 April 2025.
HDPA, 'Decision 35/2022' (13 July 2022) <https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf> accessed 28 April 2025.
HDPA, 'Decision 51/2021' (19 November 2022) <https://www.dpa.gr/sites/default/files/2021-12/51_2021anonym.pdf> accessed 28 April 2025.
HDPA, 'Decision 57/2022' (26 October 2022) <https://www.dpa.gr/sites/default/files/2023-01/57_2022%20anonym.pdf> accessed 28 April 2025.
HDPA, 'Decision 65/2018' (16 October 2018) <https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf> accessed 28 April 2025.
HDPA, 'The Authority's investigations for the TN application and for malicious software' [Έρευνες της Αρχής για εφαρμογή TN και για κακόβουλο λογισμικό] (6 February 2022) <https://www.dpa.gr/el/enimerwtiko/deltia/ereynes-tis-arhis-gia-efarmogi-tn-kai-gia-kakoboylo-logismiko> accessed 28 April 2025.
NAIH, 'Adatvédelmi hatásvizsgálati szoftver' <https://www.naih.hu/hatasvizsgalati-szoftver> accessed 6 June 2025.
NAIH, 'Decision NAIH-85/2022 (NAIH-7350/2021)' (8 February 2022) <https://www.naih.hu/data-protection/decisions?download=522:ai-based-speech-signal-processing-technology-and-data-protection> accessed 28 April 2025 [English version].
Valstybinė Doumenų Apsaugos Inspekcija, '2024. M. Veiklos Ataskaita' (2025) 17, <https://vdai.lrv.lt/public/canonical/1740980215/759/2024_m._VDAI_veiklos_ataskaita_2025_02_28_4R-104%20(1.7%20E).pdf>, accessed 30 May 2025.

Data sources and data availability

Mazur Joanna, Claudio Novelli and Zuzanna Choińska (2025, June 12) '[dataset] Should DPAs Enforce the AI Act – Data on DPAs Activities in Relation to AI,' Zenodo, https://doi.org/10.5281/zenodo.15646626.
Search of the infringement of Article 22 on GDPR Enforcement Tracker, <https://enforcementtracker.com/>, accessed 28 April 2025.
Search of the infringement of Article 22 on GDPxiv, <https://gdprxiv.org/>, accessed 28 May 2025.
Search of the infringement of Articles 22, 13(2)(f), 14(2)(g), and 15(1)(h) and for the term 'artificial intelligence' on GDPRHub, <https://gdprhub.eu/index.php?title=Advanced_Search>, accessed 28 April 2025.