Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 118

From Data Processing to Artificial Intelligence: The Evolution of EU Technology Enforcement Under the GDPR and the AI Act

Stella (Ziyu) Zhou

2025

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Stella (Ziyu) Zhou is a third-year J.D. candidate at Stanford Law School. She earned a Bachelor of Science degree from the Wharton School at the University of Pennsylvania. Coming from a business education during undergrad, she has been exploring courses, extracurricular opportunities, and topics at the intersection of business and law during her time at SLS. She will be practicing transactional law at a law firm in New York City after graduation.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Stella (Ziyu) Zhou, From Data Processing to Artificial Intelligence: The Evolution of EU Technology Enforcement Under the GDPR and the AI Act, Stanford-Vienna European Union Law Working Paper No. 118, http://ttlf.stanford.edu.

Copyright

Abstract

This paper explores the evolution of the European Union's (EU) regulatory approach to technology through a comparative analysis of the enforcement mechanisms under the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). It focuses on three elements of enforcement: regulatory authorities, sanctions and penalties, and regulatory approaches. One of the primary issues of enforcement under the GDPR is its reliance on decentralized, national authorities, which has led to inconsistent application of the law, inefficient enforcement, and limited deterrence. These challenges are likely to echo under the AI Act due to both laws' heavy reliance on national authorities. However, the AI Act introduces important structural distinctions, such as centralized enforcement for general-purpose AI via the newly established AI Office and a risk-based regulatory framework, which may improve enforcement efficiency and resource targeting. Despite these advancements, the AI Act faces its unique challenges, such as potential ambiguity in its classification system. By drawing on lessons from GDPR implementation, this paper offers early insights into the potential effectiveness and pitfalls of AI governance in the EU.

TABLE OF CONTENTS

I. INTRODUCTION

There is no question that technology plays an enormous role in our world today. In 2024, 149 zettabytes of data have been created, captured, copied, and consumed globally.[1] Among the different types of technologies, artificial intelligence (AI), in particular, has experienced exponential growth, with a dramatic surge in computing power starting around 2010.[2] AI is expected to contribute up to $15.7 trillion to the global economy in 2030, more than the combined current output of China and India, via increased productivity and consumption-side effects.[3] With the rapid development of technology comes the growing need to regulate data privacy and ensure the ethical and responsible use of emerging technologies like AI.

A. Overview of the GDPR and the AI Act

The General Data Protection Regulation (GDPR), put into effect by the European Union (EU) on May 25, 2018, regulates organizations in the EU and elsewhere that target or collect personal data of EU residents.[4] The GDPR replaced the European Data Protection Directive, which was passed in 1995, to provide modern protections that accompany the rapid technological developments and the evolution of the Internet.[5] There are two key areas that companies seeking GDPR compliance need to consider. First, Article 5 of the GDPR enumerates seven principles around which its requirements are based; they are: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and

---

[1] Kevin Bartley, *Big data statistics: How much data is there in the world?,* RIVERY (Dec.11, 2024), https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/.
[2] Peter Slattery et al., *What drives progress in AI? Trends in Compute,* FUTURETECH (Jan 3, 2025), https://futuretech.mit.edu/news/what-drives-progress-in-ai-trends-in-compute.
[3] PwC, *Sizing the prize, What's the real value of AI for your business and how can you capitalise?,* PWC'S GLOBAL ARTIFICIAL INTELLIGENCE STUDY: EXPLOITING THE AI REVOLUTION, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.
[4] Ben Wolford, *What is GDPR, the EU's new data protection law?,* GDPR.EU, https://gdpr.eu/what-is-gdpr/.
[5] *Id.*

confidentiality, and accountability.[6] Within the lawfulness principle, companies must have at least one of the six lawful bases for processing data, which are consent by data subject, performance of contract, compliance with legal obligation, protecting vital interests, carrying out of public interest or exercise of official authority, or pursuit of a legitimate interest.[7] Second, Articles 12-23 of the GDPR also set out eight individual rights over one's data, which include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights in relation to automated decision-making and profiling.[8] Certain categories of personal data are considered "sensitive" under Article 9 of the GDPR and are subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data and biometric data processed solely to identify a human being; health-related data; and data concerning a person's sex life or sexual orientation.[9] Finally, the individual data protection authorities from each of the 27 member states enforce the GDPR and levy fines on companies not compliant with the regulation.[10]

Building on the GDPR, which lays down the legal framework for governing the fundamental data protection questions, the EU put into effect the European Artificial Intelligence Act (AI Act) to specifically target the AI sector six years later on August

---

[6] *GDPR Requirements - Quick Guide on Principles & Rights,* GDPR EU, https://www.gdpreu.org/gdpr-requirements/.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 23 May 2018 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), art. 6, 2016 O.J. (L 119) 1 [hereinafter General Data Protection Regulation].

[8] *Supra* note 1.

[9] *What personal data is considered sensitive?,* EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.

[10] *The Ultimate Guide to the GDPR,* OSANO, https://www.osano.com/gdpr.

1, 2024.[11] The nature of the two regulations is different—while the GDPR is a fundamental rights law that enshrines individuals' rights when their data is being processed, the AI Act is a product safety law concerned with the safe development, deployment, and use of AI systems.[12] The two regulations are designed to work in a complementary fashion—the GDPR fills in the gaps by elucidating the individual rights one has in scenarios where an AI system processes personal data.[13] The AI Act also classifies AI systems into four risk levels and imposes different requirements depending on the risk level.[14] AI systems, like social scoring systems, are deemed to have unacceptable risks and are prohibited.[15] The next category is "high-risk" AI systems, which includes when the AI system 1) is a safety component of a product, 2) is itself a product, and 3) is referred to in an enumerated list in Annex III, which broadly encompasses AI systems in biometrics, critical infrastructure, education, employment, access to essential public and private services, law enforcement, immigration, and administration of justice and democratic processes.[16] Most of the text of the AI Act is dedicated to imposing obligations on these "high-risk" AI systems.[17] Limited-risk AI systems, such as those that interact with natural persons or generate

---

[11] Directorate-General for Communication, *AI Act enters into force,* EUROPEAN COMMISSION (Aug. 1, 2024), https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.

[12] Jane Finlayson-Brown et al., *Zooming in on AI #15, Regulatory spaghetti and AI - how to make sense of the EU GDPR and the EU AI Act,* A&O SHEARMAN (Feb. 3, 2025), https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-on-ai-14-regulatory-spaghetti-and-ai-how-to-make-sense-of-the-eu-gdpr-and-the-eu-ai-act.

[13] James Clark et al., *Europe: The EU AI Act's relationship with data protection law: key takeaways,* DLA PIPER (Apr. 25, 2024), https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/.

[14] *High-level summary of the AI Act,* EU Artificial Intelligence Act (Feb. 27, 2024), https://artificialintelligenceact.eu/high-level-summary/.

[15] *Id.*

[16] *A guide to high-risk AI systems under the EU AI Act,* PINSENT MASONS, OUT-LAW GUIDE (Feb. 13, 2024), https://www.pinsentmasons.com/out-law/guides/guide-to-high-risk-ai-systems-under-the-eu-ai-act.

[17] *Supra* note 14.

content, like chatbots and deepfakes, are subject to lighter transparency obligations.[18] Specifically, developers and deployers must ensure that end-users are aware that they are interacting with AI.[19] Finally, minimal-risk AI, such as AI-enabled video games, are unregulated.[20] Notably, the AI Act imposes separate classification rules for general-purpose AI (GPAI), and providers of GPAI have independent obligations.[21] GPAI is defined as AI models capable of performing a wide range of tasks across different domains rather than being specialized for a single application.[22] Unlike the other provisions of the AI Act that are enforced primarily by the national market surveillance authorities (MSAs), the newly established AI Office has exclusive jurisdiction over GPAI-related provisions.[23]

The GDPR is considered the most comprehensive and progressive piece of data protection legislation, and with the passing of the AI Act, the EU now has an even more thorough legal framework that has a far-reaching impact on technologies worldwide.[24]

B. Enforcement Mechanisms

Enforcement refers to the action of compelling a party to comply with a regulation, an obligation, or a judgment where it has not been complied with

---

[18] 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), art. 50, 2024 O.J. L. [hereinafter Artificial Intelligence Act]; *supra* note 14.
[19] *Supra* note 14.
[20] *Id.*
[21] *Id.*
[22] *General-purpose AI: way forward after the AI Act,* THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE (EESC) (Oct. 29, 2024), https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/general-purpose-ai-way-forward-after-ai-act.
[23] Julia Apostle, *The EU AI Act: Oversight and Enforcement,* ORRICK (Sep. 13, 2024), https://www.orrick.com/en/Insights/2024/09/The-EU-AI-Act-Oversight-and-Enforcement.
[24] *Data Protection,* EUROPEAN DATA PROTECTION SUPERVISOR, https://www.edps.europa.eu/data-protection/data-protection_en.

voluntarily within the ordered time frame.[25] Enforcement is important because, without it, regulations are rendered to mere symbolic suggestions without real regulatory effects. Some degree of legal enforcement is essential in generating and assuring compliance because it creates a credible threat that deters non-compliance and reminds and reassures parties of the need to comply.[26]

This paper examines the strengths and weaknesses of the enforcement mechanisms of the GDPR, and after conducting a comparative analysis of the enforcement structures of the GDPR and the AI Act, presents implications for the effectiveness of AI Act enforcement.

II. COMPARATIVE ANALYSIS OF ENFORCEMENT MECHANISMS UNDER THE GDPR AND THE AI ACT

This paper zooms in on three elements related to enforcement. The first is the regulatory authorities, or "who" enforces the regulations. The second is the sanctions and penalties, or "what happens" when enforcement occurs. Finally, the paper will address the regulatory approaches of the GDPR and the AI Act, or the scope and type of enforcement, which are relevant as they shed light on the effectiveness of enforcement of the AI Act as compared to that of the GDPR due to their different approaches. While there are other elements related to enforcement, such as compliance requirements and judicial review, this paper is concerned with the primary structural mechanisms that shape the effectiveness of enforcement.[27] Unlike compliance, which is a preemptive measure taken to prevent enforcement, or judicial review, which acts

---

[25] *Enforcement,* LEXISNEXIS GLOSSARY.

[26] Neil Gunningham, *Compliance, Enforcement, and Regulatory Excellence,* PENN PROGRAM ON REGULATION, 6 (2015).

[27] *See, e.g.*, General Data Protection Regulation, art. 50, 2016 O.J. (L 119) 1 (requiring providers and deployers of limited-risk AI systems to comply with certain transparency obligations); *see, e.g.*, General Data Protection Regulation, art. 78, 2016 O.J. (L 119) 1 (providing the right for an individual or a company to challenge the decision of a supervisory authority in court).

as a backstop to enforcement, the regulatory authorities, sanctions and penalties, and scope and type of enforcement delineate the outlines of the enforcement framework.

A. Regulatory Authorities

There are multiple tiers of enforcement of the GDPR, ranging from the regional level to the EU member state level, and up to the broader EU level.[28] The principal responsibilities of enforcement rest at the EU member state level. The GDPR is primarily enforced through the individual supervisory authorities (SAs), also known as the data protection authorities (DPAs), of the 27 member states.[29] DPAs are appointed by each member state and are independent of the government.[30] Under Article 58 of the GDPR, DPAs have three categories of powers: investigative, corrective, and advisory.[31] In particular, DPAs can determine if an infringement of the GDPR has occurred; issue sanctions and remedial relief, including warnings, ban on processing, and monetary fines; and support organizations or authorize specific processing activities.[32] Meanwhile, the DPAs work together on the European Data Protection Board (EDPB), which is made up of the head of each DPA and the European Data Protection Supervisor (EDPS).[33] The EDPB aims to harmonize the consistent application of the GDPR across the EU and facilitate cooperation amongst the DPAs.[34] The EDPB does not enforce the GDPR but instead provides general guidance on guidelines, recommendations, and best practices under the GDPR and adopts opinions

---

[28] Brian Daigle and Mahnaz Khan, *The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities,* JOURNAL OF INTERNATIONAL COMMERCE AND ECONOMICS, 5 (2020).
[29] *Supra* note 10.
[30] *Id; supra* note 27.
[31] General Data Protection Regulation, art. 58, 2016 O.J. (L 119) 1.
[32] European Data Protection Board, *Data Protection Authority & You,* EUROPEAN DATA PROTECTION BOARD: DATA PROTECTION GUIDE FOR SMALL BUSINESS, https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en.
[33] European Commission, *What is the European Data Protection Board (EDPB)?,* https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en.
[34] *Id.*

addressed to the European Commission or to the DPAs to advise on issues related to the GDPR.[35] However, the EDPB can issue binding decisions in one scenario—when competent DPAs do not reach a consensus in disputes regarding cross-border data processing.[36] Specifically, Article 56 of the GDPR provides for a one-stop-shop mechanism, a system of cooperation among competent DPAs, in dealing with cross-border disputes.[37] Under this mechanism, the SA or DPA of the main or single establishment of the controller or processor has competence to act as the lead supervisory authority (LSA) who makes the enforcement decision.[38] Notably, the LSA does not have exclusive competence, and other SAs or DPAs have the right to view the decision issued by the LSA.[39]

However, due to the rather decentralized enforcement structure of the GDPR, enforcement during the six years the regulation has gone into effect has suffered from problems of inconsistency and ineffectiveness. First, national interpretations and enforcement of the law have been inconsistent at times. An example of such inconsistency is the differing treatment between the Irish Data Protection Commission (DPC), Ireland's DPA that regulates a lion's share of U.S. tech companies under the GDPR, and the German, French, and other European DPAs regarding social networks' attempts to bypass user consent requirements within the EU privacy rules.[40] Shortly before the GDPR went into effect in May 2018, Meta Ireland changed its Terms of Service, which its users must accept to access Meta's Facebook and Instagram

---

[35] *About EDPB: Tasks and Duties,* EUROPEAN DATA PROTECTION BOARD, https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en.
[36] *Supra* note 32.
[37] General Data Protection Regulation, art. 56, 2016 O.J. (L 119) 1.
[38] *GDPR Enforcement Cooperation and the One-Stop-Shop: Learning from the First Three Years,* CENTRE FOR INFORMATION POLICY LEADERSHIP, 3 (2021).
[39] Yiran Lin, *More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance,* COLUMBIA JOURNAL OF TRANSNATIONAL LAW, 13 (2024).
[40] Vincent Manancourt, *'Contrary to everything we believe in': Irish data watchdog lobbied for business-friendly GDPR,* POLITICO (Dec. 5, 2021), https://www.politico.eu/article/irish-data-protection-commission-gdpr-lobby-business-friendly-general-data-protection-regulation/.

services.[41] Meta Ireland sought to rely on the "contract" legal basis for processing data under Article 6(1)(b) of the GDPR, arguing that 1) a contract was entered into between Meta and its users when the latter accepted its Terms of Service and 2) processing user data, including for personalized services and behavioral advertising, was necessary for the performance of that contract[42]. The Irish DPC initially took a lenient approach towards Meta's practice, concluding that Facebook is justified to rely on the "contract" basis to legitimize its data processing activities, including behavior advertising.[43] More broadly, the Irish DPC, through its draft opinion, explicitly pushed for social networks' ability to monitor users' behavior in order to target them with advertisements via a contract rather than via user consent.[44] The Irish DPC's draft opinion received backlash from the other European DPAs, who argued that accepting the "contract" legal basis in this case "reduces the GDPR to a pro forma instrument" and "undermines the system and spirit of the GDPR."[45] To resolve this dispute among the different DPAs, the EDPB stepped in and eventually overruled the Irish DPC's position for allowing Article 6(1)(b)'s "contractual necessity" as a lawful basis for behavioral advertising. The Irish DPC ultimately imposed a total of €390 million of administrative fines on Meta after reflecting the EDPB's binding determinations.[46] This lack of consensus among the DPAs showcases the different degrees of leniency with which different member states enforce rules under the GDPR and their inconsistent interpretations of the law.

---

[41] *Data Protection Commission announces conclusion of two inquiries into Meta Ireland,* DATA PROTECTION COMMISSION (Jan. 4, 2023), https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland.

[42] Jennifer Bryant, *Irish DPC fines Meta 390M euros over legal basis for personalized ads,* IAPP (Jan. 4, 2023), https://iapp.org/news/a/irish-dpc-fines-meta-390m-euros-over-legal-basis-for-personalized-ads.

[43] Irish Data Protection Commission, Draft Decision for the purposes of Article 60 GDPR of the Data Protection Commission made pursuant to Section 113(2)(a) of the Data Protection Act 2018, 39 (2021).

[44] *Supra* note 40.

[45] *Id.*

[46] *Supra* note 41.

Such inconsistency gives rise to the potential of forum shopping. Particularly for companies established in more than one member state and thus rely on the one-stop-shop mechanism for resolving cross-border data processing issues, there is the concern that they can forum shop and select their main establishment in a jurisdiction that best serves their commercial and regulatory interests.[47] For example, Amazon set up its EU headquarters in Luxembourg in 2003.[48] However, investigations into Amazon's management structure revealed that the tech giant's management in its Seattle headquarters granted itself permission to review and approve access to data requests for its Luxembourg unit, a task that ought to be handled by local employees.[49] An EU-based Amazon employee looking to hire team members was also told to hire into the Seattle office first even though the new recruits would be working on European matters for the Luxembourg-regulated entity.[50] These practices call into question whether Amazon Luxembourg can indeed be deemed a "main establishment" of the company.[51]

There is also a concern that the GDPR's decentralized enforcement structure caused a lack of efficiency in enforcing the regulation. This is evidenced by inefficiencies in exercising the one-stop-shop mechanism.[52] First, various DPAs have identified the use of inadequate communication tools as one of the main issues associated with the operationalization of the mechanism.[53] When working together under the one-stop-shop mechanism, the DPAs have the responsibility to provide each

---

[47] Estelle Massé, *Three Years Under The EU GDPR: An Implementation Progress Report,* ACCESS NOW, 16 (2021).
[48] About Amazon Team, "*Proud to call Luxembourg our home in Europe": Amazon celebrates 20 years in Luxembourg,* AMAZON (Sep. 20, 2023), https://www.aboutamazon.eu/news/job-creation-and-investment/proud-to-call-luxembourg-our-home-in-europe-amazon-celebrates-20-years-in-luxembourg.
[49] Vincent Manancourt, *'Millions of people's data is at risk' — Amazon insiders sound alarm over security,* POLITICO (Feb. 24, 2021), https://www.politico.eu/article/data-at-risk-amazon-security-threat/.
[50] *Id.*
[51] *Id.*
[52] *Supra* note 47.
[53] *Id.*

other with relevant information and mutual assistance to apply the GDPR consistently and facilitate effective cooperation with one another.[54] Instead of building a new tool, the EDPB level uses the Internal Market Information System, an existing system used for market monitoring in other areas of law, which an overwhelming majority of DPAs consider to be unfit for handling the high volume of complaints that have come with the GDPR.[55] The DPAs also noted a lack of clarity regarding what type of volume of information should be shared with each other via the system.[56]

Second, aside from the inconsistent interpretations of the law by the different DPAs, each member state also has different national procedures related to handling complaints, such as to what extent individuals have a right to be heard in a case, how to involve them in a case, and what information can be communicated back to them.[57] As a result, an LSA might reject a complaint even though the local authority where the case was lodged had formally accepted it.[58]

A third factor that contributes to the inefficiency is the lengthy process of coordinating among different DPAs under the one-stop shop.[59] On one hand, an inefficient LSA might become a bottleneck to the process.[60] This might happen where a DPA is constrained by resources but faces a disproportionate workload. For example, the Irish DPC received from the government an additional allocation of funding of €1.6 million for 2020, but it was less than one-third of the funding the DPC requested in its budget submission.[61] This budget shortfall pressured the DPC to reassess its

---

[54] General Data Protection Regulation, art. 61, 2016 O.J. (L 119) 1.
[55] *Supra* note 47 at 15.
[56] *Id.* at 15-16.
[57] *Id.* at 16.
[58] *Id.*
[59] *Id.* at 16-17.
[60] *Supra* note 57.
[61] *Data Protection Commission statement on increased funding of € 1.6 million in 2020 budget,* DATA PROTECTION COMMISSION (Oct. 9, 2019), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-increased-funding-eu16-million-2020.

planned expenditure for 2020.[62] In contrast to its limited budget, the Irish DPC, which acts as the LSA for many tech multinationals with European headquarters in Ireland, received 7,000 complaints, almost 5,000 breach notifications, and has been contacted by the public and different organizations seeking guidance over 40,000 times during ten months in 2019.[63] On the other hand, the long lead time for the concerning supervisory authorities (CSAs) to transmit information can delay the efficiency of the LSA. For instance, the Irish DPC reported several instances in the first year of cooperation under the GDPR where a CSA could take several months to transmit complaint files to the DPC as the LSA, which led to months-long delays in the handling of complaints.[64]

At times, it is also difficult to identify the LSA in a cross-border issue.[65] In particular, it is unclear how DPAs assess whether the main establishment of a company is indeed where it makes real and effective management decisions regarding data processing.[66] This is problematic as large tech companies might abuse this situation to cherry-pick their desired jurisdiction to resolve cross-border cases, as illustrated by the Amazon Luxembourg example above.

Finally, officials and privacy specialists around Europe have elicited the general criticism that LSAs lean heavily toward "engagement," or advising companies on how to stay legal, over investigations and enforcement.[67]

---

[62] *Id.*
[63] *Id.*
[64] Irish Supervisory Authority, *Evaluation of the GDPR Under Article 97 — Questions to Data Protection Authorities / European Data Protection Board: Answers from the Irish Supervisory Authority,* GENERAL DATA PROTECTION BOARD, 3 (2019).
[65] *Supra* note 47 at 17-18.
[66] *Id.*
[67] Nicholas Vinocur, *'We have a huge problem': European regulator despairs over lack of enforcement,* POLITICO (Dec. 27, 2019), https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/.

This lack of efficiency in the enforcement of cross-border cases has been picked up by the European Commission, which proposed additional procedural rules relating to cross-border GDPR enforcement in July of 2023.[68] For example, the additional rules will introduce a new obligation for the LSA to send a "summary of key issues" to their counterparts, which is aimed at facilitating communication and consensus among the CSAs during the initial stages of the process.[69] The adoption of these new procedural rules will likely enhance the effectiveness of the one-stop-shop mechanism in resolving cross-border disputes.

Similar to the GDPR, the AI Act is also being enforced primarily at the level of the EU member states. Each EU member state must appoint or establish at least one market surveillance authority and one notifying authority to enforce the AI Act, except for the GPAI-related provisions.[70] The MSAs have enforcement power. In particular, they can require providers, deployers, and importers of AI systems to provide relevant data for assessing the AI system's compliance, take measures to bring non-compliant systems into compliance, or otherwise impose sanctions on non-compliant systems.[71] Notifying authorities, on the other hand, establish and perform the procedure for assessment, designation, notification, and monitoring of conformity assessment bodies, who certify the compliance of high-risk AI systems with the AI Act.[72] Unlike the MSAs, notifying authorities do not have the power to impose sanctions for non-

---

[68] European Commission Press Release (IP/23/3609), Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases (Jul. 4, 2023).
[69] *Id.*
[70] Christoph Werkmeister et al., *EU AI Act Unpacked #9: Who are the regulators to enforce the AI Act?,* FRESHFIELDS (Jul. 4, 2024), https://technologyquotient.freshfields.com/post/102jc22/eu-ai-act-unpacked-9-who-are-the-regulators-to-enforce-the-ai-act.
[71] *Id.*
[72] *Overview of all AI Act National Implementation Plans,* EU ARTIFICIAL INTELLIGENCE ACT (Nov. 8, 2024), https://artificialintelligenceact.eu/national-implementation-plans/; Dr. Catherine Di Lorenzo et al., *Zooming in on AI - #14: Enforcement of the AI Act,* A&O SHEARMAN (Feb. 4, 2025), https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-on-ai-14-enforcement-of-the-ai-act.

compliance.[73] Together, the market surveillance authority and the notifying authority are referred to as the national competent authorities.[74] Additionally, where non-compliance extends beyond one national territory, an MSA must communicate and cooperate with other member states, similar to how the DPAs cooperate under the one-stop-shop mechanism in resolving cross-border issues.[75] The European Artificial Intelligence Board (AI Board), composed of one representative per member state, facilitates cooperation and harmonizes the application of the AI Act across member states.[76] This is similar to the role of the EDPB under the GDPR.

Because the enforcement of the AI Act also largely relies on the national authorities, the AI Act might suffer from a similar problem of inconsistent enforcement like the GDPR. The MSAs bear many similarities to the DPAs under the GDPR—both have the power to conduct investigations, order corrective actions, impose penalties for non-compliance, and ban or restrict certain activities. Where there are different national procedures, legal interpretations, and priorities, there might be a lack of harmonization on how different member states are interpreting, applying, and enforcing the AI Act.[77] Additionally, the MSAs of different member states might have differing levels of expertise.[78] The AI Act afforded each member state wide discretion regarding the structure and design of their respective MSA.[79] For example, Spain has established a single MSA under the Spanish Department of Digital Transformation, whereas Finland has proposed a much more decentralized model consisting of 10

---

[73] Dr. Catherine Di Lorenzo et al., *Zooming in on AI - #14: Enforcement of the AI Act,* A&O SHEARMAN (Feb. 4, 2025), https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-on-ai-14-enforcement-of-the-ai-act.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Supra* note 72.

existing MSAs, such as the Energy Authority and the Medicines Agency.[80] This variation in institutional background and structure will likely further widen the gap of enforcement across member states. Finally, with regard to resolving cross-border issues, the AI Act's enforcement structure is even more decentralized than that of the GDPR as it lacks the one-stop-shop mechanism.[81] Granted, as discussed above, the one-stop shop was not as efficient in practice, but not setting up such a mechanism, to begin with, might pose even greater administrative burdens from dealing with multiple national authorities.[82] Finally, to what extent the problems of inconsistency and inefficiency in enforcing the GDPR will transfer to that of the AI Act will also depend on factors like the sufficiency of funding to the national MSAs.

However, the inconsistency and inefficiency problems that emerged under the GDPR will likely be ameliorated with regard to enforcing the GPAI-related provisions under the AI Act. Article 88 of the AI Act vests in the European Commission the exclusive powers to supervise and enforce the GPAI-related provisions, and the Commission in turn established the new AI Office within its structure to enforce these provisions.[83] Under the GDPR, the most analogous centralizing authority is the EDPB. However, the EDPB has no enforcement power other than issuing binding decisions to settle cross-border data processing disputes among DPAs.[84] Additionally, this power only comes in when the national authorities, the first line of enforcers, have already exercised their enforcement powers but cannot reach a consensus. In other words, the enforcement power still largely rests with the national level under the GDPR. In contrast, the AI Act creates a strict hierarchy of authority as to the GPAI-related provisions as the MSAs cannot independently enforce the GPAI-related provisions or

[80] *Id.*
[81] *Supra* note 73.
[82] *Id.*
[83] Artificial Intelligence Act, art. 88, 2024 O.J. L; *supra* note 23.
[84] *Supra* note 32.

override the decision of the AI Office. Thus, because only one authority is making the enforcement decision, and the authority sits at the broader EU level, there won't be room for inconsistent enforcement or a lack of effective cooperation among the national authorities like that in the GDPR.

B. Sanctions and Penalties

Both the GDPR and the AI Act levy hefty fines for non-compliance. The GDPR has a two-tiered structure for administrative fines.[85] For less severe infringements, the GDPR imposes a fine of up to €10 million, or in the case of an undertaking, up to 2% of the firm's worldwide annual turnover from the preceding financial year, whichever is higher.[86] This tier includes violations of the articles governing the obligations of the controllers and processors, the certification body, and the monitoring body.[87] More severe infringements are subject to a fine of up to €20 million, or in the case of an undertaking, up to 4% of the firm's worldwide annual turnover from the preceding financial year, whichever is higher.[88] They include violations of the articles governing the basic principles of processing, including conditions for consent, the data subjects' rights, the transfer of data to an international organization or a recipient in a third country, any violation of member state laws adopted under Chapter IX, and non-compliance with an order by a supervisory authority.[89]

The GDPR also provides for non-monetary sanctions. Instead of or in addition to imposing a fine, DPAs have other corrective powers, including forcing the controllers and processors to grant data subjects their rights, ordering them to bring processing operations into compliance within a specified period, imposing a temporary

[85] General Data Protection Regulation, art. 83, 2016 O.J. (L 119) 1.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*

or permanent ban on processing, and suspending data flows to a recipient in a third country, etc.[90]

Despite the gravity of the administrative fines, some evidence suggests they have not achieved the desired degree of deterrent and corrective effects.[91] The first issue is the lack of harmonization in the imposition and calculation of fines.[92] This inconsistency is largely due to the EU member state-driven enforcement structure of the GDPR, as discussed above. The DPAs exhibit a huge disparity in the number and amount of fines imposed.[93] From May 2018 to May 2021, a total of 2208 fines were imposed, more than half of which were imposed by three DPAs—Germany (606), Spain (279), and Italy (228).[94] Meanwhile, seven DPAs, including Ireland and Luxembourg which house the headquarters of many U.S. Big Tech companies, imposed less than 10 fines during the same three-year period.[95] One explanation for this is the disparity of resources across the different DPAs. According to a 2022 report published by the EDPB, 77% of the DPAs considered their allocated budget insufficient to carry out their activities.[96] The amount of human capital also varies widely—while German DPAs employ close to 1,200 staff members, Belgian, Croatian, and Romanian DPAs average only 50.[97] This gap in resources is linked to the DPAs'

---

[90] General Data Protection Regulation, art. 58, 2016 O.J. (L 119) 1.

[91] *See generally* Mona Naomi Lintvedt, *Putting a price on data protection infringement,* 12 INT'L DATA PRIVACY L.J. 1 (2021), https://academic.oup.com/idpl/article/12/1/1/6453860.

[92] *Id* at 5-9.

[93] *Id* at 5.

[94] *Id.*

[95] Jenny Egnér Lin, *Facebook, Google, LinkedIn - Why do all major tech companies place their European headquarters in Dublin?,* EUROPEAN HIGHER EDUCATION FAIR (Mar. 24, 2025), https://ehef.id/post/facebook-google-linkedin-why-do-all-major-tech-companies-place-their-european-headquarters-dublin/en; Rémy Cornet, *Four reasons why companies incorporate in Luxembourg,* OCORIAN (Jul. 18, 2023), https://www.ocorian.com/insights-news-press-releases/four-reasons-why-companies-incorporate-luxembourg; *Id.*

[96] *Overview on resources made available by Member States to the Data Protection Supervisory Authorities,* EUROPEAN DATA PROTECTION BOARD, 5 (2022).

[97] Anda Bologa, *Fifty Shades of GDPR Privacy: The Good, the Bad, and the Enforcement,* CENTER FOR EUROPEAN POLICY ANALYSIS, (Feb. 7, 2023), https://cepa.org/article/fifty-shades-of-gdpr-privacy-the-good-the-bad-and-the-enforcement/.

differing determination to levy fines.[98] Furthermore, for a few years after the GDPR was put into effect, the only guideline adopted by the EDPB on administrative fines only discussed general guiding principles, such as requiring the fines to be "effective, proportionate and dissuasive."[99] The lack of specific guidelines led the DPAs to use their own methods to calculate the fines.[100] For example, "turnover" was calculated differently—the Irish DPA, in their case against Twitter, used the revenue in the firm's annual report for the preceding year, while the Norwegian DPA, in their case against Grindr, relied on online articles about the firm's revenue and profit as a proxy to the turnover without referring to its annual report.[101] Going forward, this inconsistency in calculating the fines will likely be mitigated as the EDPB adopted a new, more specific guideline on the calculation of administrative fines under the GDPR in May of 2023, which provided a precise definition for "turnover," among its other detailed instructions.[102]

A second issue that weakens the deterrent effect of the fines is the lack of transparency in the outcome of the DPAs' decisions.[103] The GDPR empowers the DPAs to publish the outcomes of their decisions via provisions such as Article 59, which indicates the possibility of including "a list of types of infringement notified and types of measures taken" in the DPAs' annual report on their activities.[104] However, nowhere in the GDPR mandates such publication.[105] This has led to varying degrees of

---

[98] *Id.*

[99] European Commission, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253 (2017), https://ec.europa.eu/newsroom/article29/items/611237.

[100] *Supra* note 91 at 6.

[101] Irish Data Protection Commission, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018, 181 (2020); Norwegian Data Protection Authority, Advance notification of an administrative fine, 27 (2021).

[102] *See generally* European Commission, Guidelines 04/2022 on the calculation of the administrative fines under the GDPR (May 24, 2023).

[103] *Supra* note 91 at 9-11.

[104] General Data Protection Regulation, art. 59, 2016 O.J. (L 119) 1

[105] *Supra* note 91 at 9.

transparency across the DPAs. For example, persons who work for the National Data Protection Commission (CNPD) of Luxembourg, the DPA of the jurisdiction, are subject to obligations of professional secrecy, and thus the CNPD refrains from publishing draft decisions on administrative fines in adherence to this requirement.[106] In contrast, the Belgium DPA publishes its decisions for transparency but decides on a case-by-case basis whether to identify the parties involved.[107] This lack of transparency in some cases weakens the educational effect of enforcement and the deterrent effect of administrative fines.[108]

Finally, the efficacy of the administrative fines is tied to the efficiency with which DPAs investigate and enforce sanctions and penalties against non-compliance under the GDPR. As discussed above, the Irish DPC has faced criticism for its slow enforcement of the GDPR, having been considered as the "big EU bottleneck" in cross-border cases.[109] For instance, the Irish DPC launched an inquiry into Meta Platforms Ireland Limited launched in April 2019 but did not reach a final decision until September 2024.[110] The GDPR lacks salience to the companies subject to its obligations due to the long delays, as shown above, between the instance of infringement and enforcement by the respective DPA, and such delays thereby diminish the deterrent effect of the regulation.

The AI Act imposes even more onerous administrative fines than the GDPR. The AI Act's monetary penalty provisions target three actors.[111] First, any violation of

---

[106] Loi du 1er août 2018, Section IX, Secret professionnel, Art. 42, Mémorial A, 2018, No. 686 (Lux.).
[107] Autorité de protection des données, *Politique de publication des décisions de la Chambre contentieuse,* 3 (2020); *supra* note 91 at 10.
[108] *Supra* note 91 at 9.
[109] Johnny Ryan and Alan Toner, *Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities,* IRISH COUNCIL FOR CIVIL LIBERTIES, 5 (2021).
[110] *Irish Data Protection Commission fines Meta Ireland €91 million,* DATA PROTECTION COMMISSION (Sep. 27, 2024), https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta?utm_source=chatgpt.com.
[111] Artificial Intelligence Act, art. 99-101, 2024 O.J. L.

the AI Act by operators of AI systems is subject to a three-tiered penalty system: 1) non-compliance with the prohibition of AI practices referred to Article 5, such as social scoring, is subject to fines up to €35 million, or if the offender is an undertaking, up to 7% of the total worldwide annual turnover for the preceding financial year, whichever is higher; 2) non-compliance with provisions related to operators or notified bodies are subject to fines up to the higher of €15 million or 3%; and 3) the supply of incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply to a request is subject to fines of up to the higher of €7.5 million or 1%.[112] Second, any violations by providers of GPAI models are subject to fines up to the higher of €15 million or 3% of their annual total worldwide turnover.[113] Finally, violations by union institutions, bodies, offices, and agencies are subject to a two-tiered fine system: 1) non-compliance with the prohibition of AI practices is subject to fines of up to €1.5 million; 2) non-compliance with other AI systems is subject to fines of up to €750,000.[114]

Like the GDPR, the AI Act also empowers MSAs to impose non-monetary sanctions. Where the MSA finds non-compliance by an AI system, it can 1) order all appropriate corrective actions to bring the AI system into compliance or 2) withdraw or recall the AI system from the market; or where the operator fails to bring the system into compliance, 1) prohibit or restrict the AI system from being made available in its national market or put into service or 2) withdraw or recall the product or the standalone AI system from the market.[115]

Except for the GPAI-related provisions, the AI Act is largely being enforced by national authorities in each EU member state, so it is likely to face a similar

[112] Artificial Intelligence Act, art. 99, 2024 O.J. L.
[113] Artificial Intelligence Act, art. 101, 2024 O.J. L.
[114] Artificial Intelligence Act, art. 100, 2024 O.J. L.
[115] Artificial Intelligence Act, art. 79(2), (5), 2024 O.J. L.

inconsistency problem as the GDPR. Similar to the text of the GDPR, the AI Act provides general guiding principles that penalties, including administrative fines, shall be "effective, proportionate and dissuasive."[116] However, no further guidelines detailing the methodology for calculating fines under the AI Act have been issued. This means that each DPA is not bound to use a certain base figure or fixed financial starting point for assessing the proposed fine and can devise its own methodology, which creates the potential for inconsistency.[117]

Likewise, the AI Act does not mandate disclosure of enforcement decisions by MSAs. Thus, it is likely that the national authority of each member state will exercise varying degrees of transparency regarding their enforcement decisions.

While the AI Act and the GDPR have comparable levels of fines, the AI Act imposes a higher ceiling of fine, €35 million or 7% annual turnover, compared to GDPR's €20 million or 4% annual turnover, for the most severe infringements.[118] However, if the problems of inconsistency and lack of transparency persist in the imposition of penalties under the AI Act, it is questionable whether the higher fine threshold will indeed achieve a larger deterrent effect. Furthermore, it is important to consider the financial resources of the Big Tech companies—those who are the most frequent targets of the enforcement actions—when assessing the onerousness of the fines. So far, the biggest fine levied under the GDPR was the €1.2 billion fine imposed on Meta by the Irish DPC in 2023.[119] While this is a high absolute number, Meta

---

[116] *Supra* note 113.

[117] *See supra* note 101 (The Irish DPC remarked that due to the absence of EU-level guidelines on the calculation of finds, "[it is] not bound to use a base figure or fixed financial starting point for the assessment of the proposed fine.").

[118] *Supra* note 113; *supra* note 85.

[119] *20 biggest GDPR fines so far [2025],* DATA PRIVACY MANAGER (Mar. 3, 2025), https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/.

earned $134.902 billion, or roughly €123.29 billion, in revenue in the same year.[120] Put into perspective, the fine levied amounted to less than 1% of Meta's annual revenue, which is less than the floor of 2% for less severe infringements under the GDPR.[121] The ample financial resources of the Big Tech companies also enable them to carry out drawn-out legal battles.[122] In Ireland, for example, as long as the offending company invokes its statutory right to appeal, the decision of the Irish DPC will not be confirmed by the Circuit Court, the latter being the necessary step for the fine levied to become payable.[123] This is precisely what happened—Of the total close to €3 billion GDPR fines issued by the Irish DPC between 2020 and the end of October 2024, just around €18 million, or 0.6% have been paid as of December 2024.[124] The deterrence effect of fines does not kick in until the fines have been actually paid.[125] This all calls into question whether the administrative fines, although seemingly hefty, actually pose a credible threat to the tech companies that are the most desirable targets, or if they have in practice been rendered to simply a mandatory entry fee in order to operate in the EU.

C. Scope and Type of Enforcement

Both the GDPR and the AI Act have an extraterritorial scope. Under the GDPR, controllers and processors not established in the EU can be subject to the regulation as long as they perform two types of processing activities related to subjects

---

[120] Press Release, Meta Platforms, Inc., *Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend* (Feb. 1, 2024), https://investor.atmeta.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx.
[121] *Supra* note 85.
[122] James Coker, *Deterring Data Privacy Violations in Big Tech: Why Fines Are Not Enough,* INFOSECURITY MAGAZINE (Jan. 28, 2025), https://www.infosecurity-magazine.com/news-features/data-privacy-violations-big-tech/.
[123] *Id.*
[124] *Id.*
[125] *Id.*

in the EU.[126] This happens when they either intend to offer goods or services to or monitor the behavior of an individual located in the EU.[127] Likewise, the AI Act also targets certain organizations located outside the EU where they place on the market or put into service AI systems or GPAI models, or where the output produced by their AI systems is used by persons in the EU.[128]

However, the GDPR and the AI Act differ substantially in their regulatory approaches. The GDPR is technology-neutral as it protects personal data regardless of the technology used for processing it.[129] Except for Article 9, which prohibits the processing of certain categories of data, such as racial or ethnic origin and political opinions, and Article 35, which requires the carrying out of a data protection impact assessment for certain types of processing likely to result in a high risk to the rights and freedoms of persons, its rules apply broadly to all kinds of data processing.[130] In comparison, the AI Act takes a risk-based regulatory approach and imposes different rules on AI systems based on their risk level.[131]

The comparison of the different regulatory approaches sheds light on the regulatory intent and potential enforcement effectiveness of the AI Act. First, the risk-based approach of the AI Act will likely facilitate a more targeted use of regulatory resources. Due to the broad application of the GDPR, DPAs have to direct their attention to all kinds of infringements, regardless of their severity, including minor infringements such as a bank failing to erase an incorrect phone number of a data subject despite their request and thus violating the principle of accuracy under the

---

[126] General Data Protection Regulation, art. 3, 2016 O.J. (L 119) 1.
[127] European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (Nov. 12, 2019).
[128] Artificial Intelligence Act, art. 2, 2024 O.J. L.
[129] European Commission, *Data protection explained,* https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.
[130] General Data Protection Regulation, art. 9, 35, 2016 O.J. (L 119) 1.
[131] *Supra* note 14.

GDPR.[132] In comparison, most of the obligations under the AI Act fall on the high-risk AI systems, which allows the MSAs to focus their resources on AI systems with the greatest potential for harm.[133] This might help shorten the delay between infringement and enforcement, one of the major problems under the GDPR, especially given jurisdictions like Ireland with limited resources but considerable regulatory burdens.

Meanwhile, the AI Act's risk-based approach might also introduce regulatory ambiguity. First, the risk-based approach introduces the burden of classification. An example of such ambiguity is the classification of an AI-based medical device undergoing clinical investigations.[134] Under the AI Act, an AI system that is used as a safety component of a medical device or is a device itself is considered a high-risk AI system.[135] However, it is unclear whether the medical device would be considered being "placed on the market," a condition that brings the device under the purview of the AI Act, during the clinical investigation phase.[136] On one hand, the definition of "placing on the market" under the AI Act does not contain an exemption for an AI system during clinical investigation.[137] On the other hand, the entire AI Act does not apply to "any research, testing or development activity regarding AI systems," which might encompass this scenario.[138] Thus, regulatory authorities will likely expend more efforts grappling with these nuanced classification rules under the AI Act.

The definition of "AI systems" might also introduce ambiguity. Notably, in the initial proposal of the AI Act circulated in 2021, the European Commission defined

---

[132] *Hungary fine two companies for GDPR infringement,* CMS LAW-NOW (Aug. 3, 2019), https://cms-lawnow.com/en/ealerts/2019/03/hungary-fines-two-companies-for-gdpr-infringement.
[133] *Supra* note 14.
[134] *See generally* Arne Thiermann and Hannah Wiborg, *Call for Action: How does the AI Act apply to clinical investigations of AIMD?,* HOGAN LOVELLS (Oct 2024).
[135] Artificial Intelligence Act, art. 1, 2024 O.J. L; Artificial Intelligence Act, Annex. 1, 2024 O.J. L; *id.* at 4.
[136] Artificial Intelligence Act, art. 5, 2024 O.J. L.
[137] Artificial Intelligence Act, art. 3(9), 2024 O.J. L.
[138] Artificial Intelligence Act, art. 2(8), 2024 O.J. L.

"AI system" as software developed with one or more of the specifically enumerated techniques and approaches.[139] However, in the final version, the Commission shifted to a broader definition, likely with the intention of maintaining the long-term applicability of the AI Act to technologies and methods that have not yet been developed. [140] This more expansive definition will likely also create additional regulatory responsibilities of determining whether certain future innovations qualify as "AI systems" and thus fall under the purview of the AI Act. That said, the final version of the AI Act did retain a list-based approach in other areas, such as in providing a list of use cases that will be defined as "high-risk AI."[141] During the legislative process, the European Economic and Social Committee cautioned against using such an approach, arguing that the list left out and thereby legitimized a number of heavily criticized AI systems.[142] Nevertheless, retaining this list-based approach in the final adoption of the AI Act reflects the EU's preference for regulatory clarity. Taken together with the inclusive definition of an "AI system," the EU seems to be striking a balance between achieving the clarity of regulation and maintaining the Act's future applicability in the face of rapid technological growth.

III. CONCLUSION

Overall, the GDPR and the AI Act share many regulatory similarities. They both rely largely on the national authorities of each EU member state to enforce the

---

[139] European Commission, Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

[140] *See* Artificial Intelligence Act, art. 3, 2024 O.J. L (defining "AI System" as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.").

[141] *See* Artificial Intelligence Act, Annex. 3, 2024 O.J. L.

[142] European Economic and Social Committee, Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, INT/940.

regulations, impose heavy administrative fines on non-compliant organizations, and are extraterritorial in scope. Because of these similarities, the AI Act will likely face many similar problems as the GDPR in its enforcement, the most notable one being inconsistent enforcement across the EU member states due to their different interpretations of the law, legal procedures, budget and resources, caseload, and calculation and imposition of sanctions and penalties. The AI Act is also set up to have more efficient enforcement than the GDPR in some ways, including creating the new AI Office to allow EU-level enforcement for GPAI-related provisions and using a risk-based approach that prioritizes the regulation of AI systems carrying the most potential harm. Meanwhile, the AI Act carries its unique challenges, such as potentially requiring more regulatory effort in classifying and defining AI systems, though this is understandably a tradeoff in creating a piece of regulation that aims to stay relevant in the long term in a society where AI-driven technological changes are occurring at a high velocity every day. This paper has performed a comparative analysis between the enforcement mechanisms of the GDPR and the AI Act. It has also drawn relevant and notable implications about the enforcement of the AI Act from the existing problems and criticisms of GDPR enforcement. Given the nascent nature of the AI Act, it remains to be seen as cases emerge and further guidelines are adopted how its enforcement mechanisms will be executed in practice.