AI & Partners

Amsterdam - London - Singapore

EU AI Act

GDPR Enforcement Tracker

Enforcing the EU AI Act with Fines

May 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Jean NG, AI Changemaker

Mehmet Tahir Agrak

Erdinc Sacan, Fontys University

Peter Slattery, MIT

AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Contents

Introduction

As artificial intelligence continues to reshape industries, the need for robust regulatory frameworks to safeguard data privacy has never been more critical. Emerging AI regulations, including the EU AI Act and updates to GDPR enforcement, aim to ensure that AI systems operate transparently, ethically, and in compliance with stringent data protection standards. These regulatory measures impose new obligations on organizations, requiring them to assess AI risks, implement accountability mechanisms, and enhance data governance practices.

This report examines the intersection of AI regulation and data protection, offering insights into how evolving legal frameworks shape AI deployment. From mandatory impact assessments to data minimization requirements, AI governance now demands a proactive approach to mitigating privacy risks and ensuring compliance. Organizations must navigate complex regulatory landscapes to maintain consumer trust and avoid significant penalties.

With increasing scrutiny from global regulators, businesses must demonstrate AI governance maturity by integrating privacy-preserving technologies, enhancing transparency, and adopting responsible AI practices. Effective compliance strategies not only reduce legal exposure but also strengthen consumer confidence in AI-driven systems.

Whether you are an AI developer, enterprise leader, or policymaker, this report provides strategic guidance on aligning AI operations with emerging data protection regulations. At AI & Partners, we are committed to supporting organizations in building AI systems that prioritize privacy, security, and regulatory compliance in an increasingly complex legal environment.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about insights on forecasted EU AI Act fines drawn from GDPR Enforcement Data

1. What can GDPR enforcement trends tell us about future EU AI Act fines?

GDPR enforcement data suggests that AI Act fines will be significant in both scale and frequency, particularly in sectors with a history of non-compliance like finance, media, and healthcare. Regulators will likely mirror GDPR practices: penalizing failures in consent, transparency, and data security. Organizations repeatedly fined under GDPR may face compounded penalties under the AI Act. The overlap in principles—like data minimization, purpose limitation, and accountability—means past enforcement is a strong predictor of future risk. Companies should expect AI Act enforcement to adopt a similarly firm, principle-based, and risk-sensitive approach.

2. Which sectors are most vulnerable to high AI Act fines based on GDPR patterns?

Sectors heavily fined under GDPR—such as finance, telecommunications, healthcare, media, and public administration—are similarly vulnerable under the AI Act due to their use of high-risk AI systems and sensitive data. These industries often handle biometric, profiling, or large-scale personal data that triggers stricter regulatory scrutiny. Violations in transparency, consent, and algorithmic fairness are particularly common. The EU AI Act amplifies risk where AI is used in critical decisions like credit scoring, recruitment, or patient diagnosis. Thus, sectors with repeated GDPR violations should prepare for intensified oversight and more severe consequences under the AI Act.

3. How will enforcement differ between large enterprises and SMEs under the EU AI Act?

GDPR enforcement has shown regulators tailor fines to organizational size and financial capacity, a principle expected to continue under the AI Act. While large enterprises face multimillion-euro fines and structural oversight obligations, SMEs may receive smaller penalties but still face heavy administrative burdens, such as mandatory documentation or audits. Importantly, SMEs using high-risk AI—especially in surveillance or decision-making—will not be exempt from enforcement. Regulators aim for proportionality, not exemption. Thus, even smaller firms must take compliance seriously to avoid cumulative sanctions, reputational damage, or mandated system shutdowns that could significantly disrupt operations.

4. What specific AI practices are likely to trigger enforcement under the AI Act?

Practices likely to attract enforcement include the use of opaque, discriminatory, or unexplainable algorithms; biometric surveillance without clear consent; AI systems that lack human oversight; and those deployed without prior risk assessment. Under GDPR, similar behaviours—like unlawful processing or profiling—have been key reasons for fines. The AI Act adds layers of accountability, including mandatory documentation, transparency obligations, and post-deployment monitoring. Any failure to demonstrate system reliability, bias mitigation, or user rights protections could result in enforcement. Systems used in employment, law enforcement, healthcare, and education are especially at risk if these practices are not followed.

5. How can organizations use GDPR fine data to forecast AI Act exposure?

Analysing GDPR enforcement data—such as fine amounts, violation types, and affected sectors—helps identify regulatory priorities. For example, frequent GDPR fines for video surveillance, improper consent, or insecure processing suggest AI systems using these techniques will be highly scrutinized. Firms can map this historical data to their current AI use to forecast enforcement hotspots. Reviewing which GDPR articles were violated (e.g., Articles 5, 6, 32) also reveals which AI governance areas need attention. This predictive approach allows firms to proactively audit AI systems, plug compliance gaps, and prioritize risk areas before enforcement escalates under the AI Act.

6. What role will data protection authorities (DPAs) play in AI Act enforcement?

DPAs, experienced through GDPR enforcement, will be central to EU AI Act implementation. Their institutional knowledge, staffing, and sector focus—documented in GDPR fine reports—provide insight into their likely AI oversight behaviours. Countries like France, Germany, and Spain, with assertive GDPR enforcement records, are expected to lead in issuing AI Act fines. DPAs will evaluate AI governance frameworks, inspect documentation, and assess compliance with transparency and risk management requirements. Their ability to impose corrective measures, suspend systems, or mandate audits will be amplified. Thus, DPAs' GDPR behaviour offers a clear blueprint for how they'll enforce AI-specific rules.

7. What are common compliance failings that led to GDPR fines and may trigger AI Act penalties?

Typical GDPR violations include lack of legal basis for data processing, inadequate transparency, missing data protection impact assessments (DPIAs), poor cybersecurity, and insufficient user consent. These same issues will be penalized under the AI Act, especially where AI systems are involved in sensitive decision-making. For instance, failure to explain how an AI system makes decisions can violate both GDPR's fairness and AI Act's transparency obligations. Organizations also often lacked robust documentation or failed to demonstrate compliance measures—an AI Act red flag. Repeating these errors in AI contexts is likely to provoke fines, audits, or enforced system redesigns.

8. How high can EU AI Act fines go, and what factors influence their size?

AI Act fines can reach up to **€35 million** or **7%** of global annual turnover, surpassing GDPR's 4%. Factors influencing fine size include the nature and severity of the infringement, whether it was intentional or negligent, the categories of data affected (e.g., sensitive or biometric), and prior compliance history. GDPR enforcement data shows that repeated violations, large-scale impact, or obstructing investigations sharply increase penalties. The same will apply under the AI Act. Documentation quality, transparency, and organizational cooperation with authorities will influence outcomes. Businesses that ignore early warnings or fail to rectify risks may face maximum-tier fines.

9. Will countries enforce the AI Act uniformly, or will some be stricter?

Just as GDPR enforcement varies by country, AI Act enforcement will reflect national differences in resources, regulatory priorities, and legal systems. Countries like France, Italy, Germany, and Spain have demonstrated aggressive GDPR enforcement and are expected to maintain that stance under the AI Act. Conversely, nations with lower fine volumes or transparency—like Croatia or Czech Republic—may adopt more cautious approaches. Factors such as regulator staffing, political support, and local industry dynamics will influence enforcement intensity. Organizations operating across borders must prepare for regulatory fragmentation and adopt high standards to meet the strictest enforcement jurisdiction's expectations.

10. What proactive steps can organizations take to avoid AI Act fines?

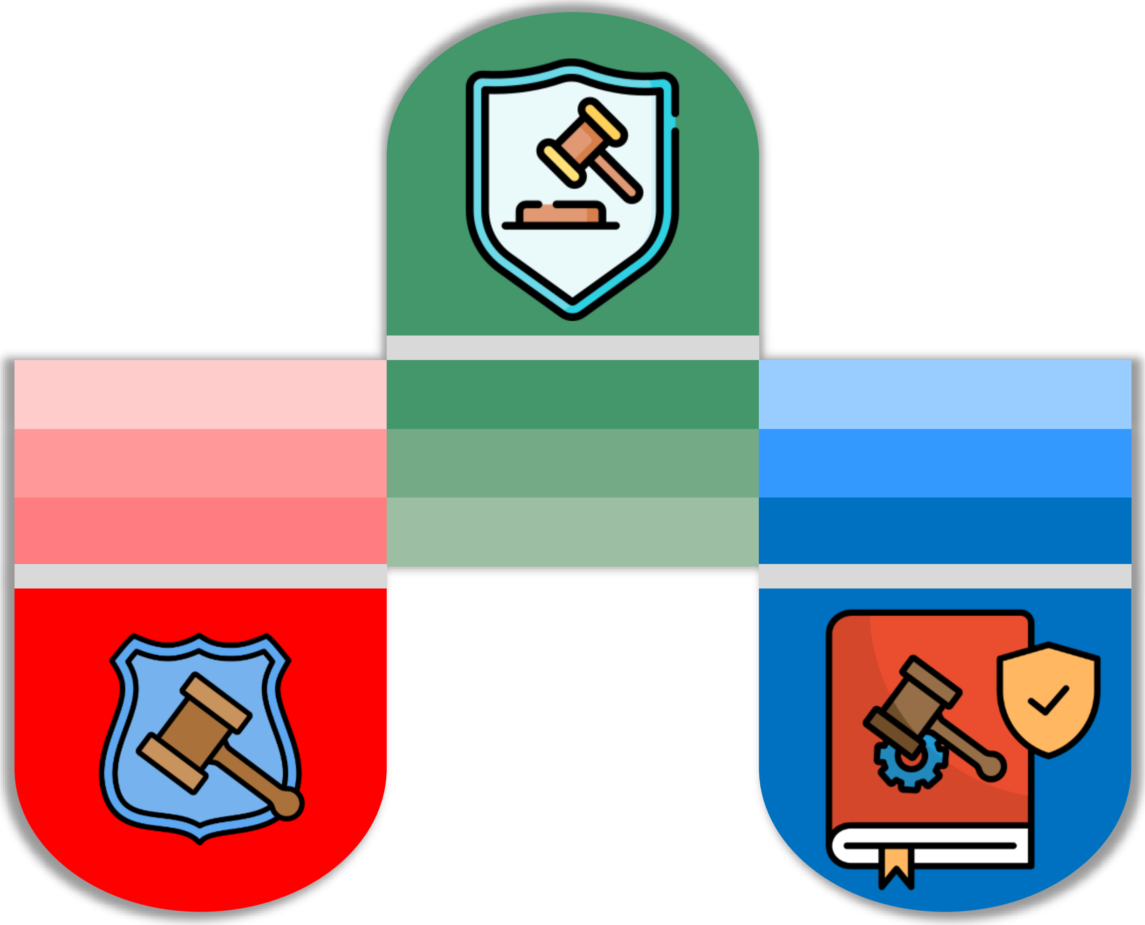
To avoid AI Act fines, organizations should immediately map their AI use cases, assess risk levels, and document system design, data flows, and decision logic. Conducting thorough impact assessments—akin to GDPR's DPIAs—is vital. Embedding privacy-by-design, bias mitigation, and explainability into AI systems can reduce liability. Regular third-party audits, staff training, and real-time compliance monitoring help demonstrate diligence. Aligning with existing frameworks like ISO/IEC 42001 or NIST AI RMF can also show good faith. Most importantly, firms should ensure they can transparently explain and justify any AI decision that affects individuals—especially in high-risk contexts like healthcare or employment.

Understanding insights on forecasted EU AI Act fines drawn from GDPR Enforcement Data

Core Insights

Why will it happen in these areas?

These sectors present elevated risks due to complex AI use, systemic data handling, and prior GDPR violations. Regulators prioritize them for their potential to infringe on fundamental rights, enable discrimination, or compromise security. High-profile breaches and opaque algorithmic decisions in these industries have already drawn regulatory scrutiny and big fines.



Where will EU AI Act enforcement action likely arise?

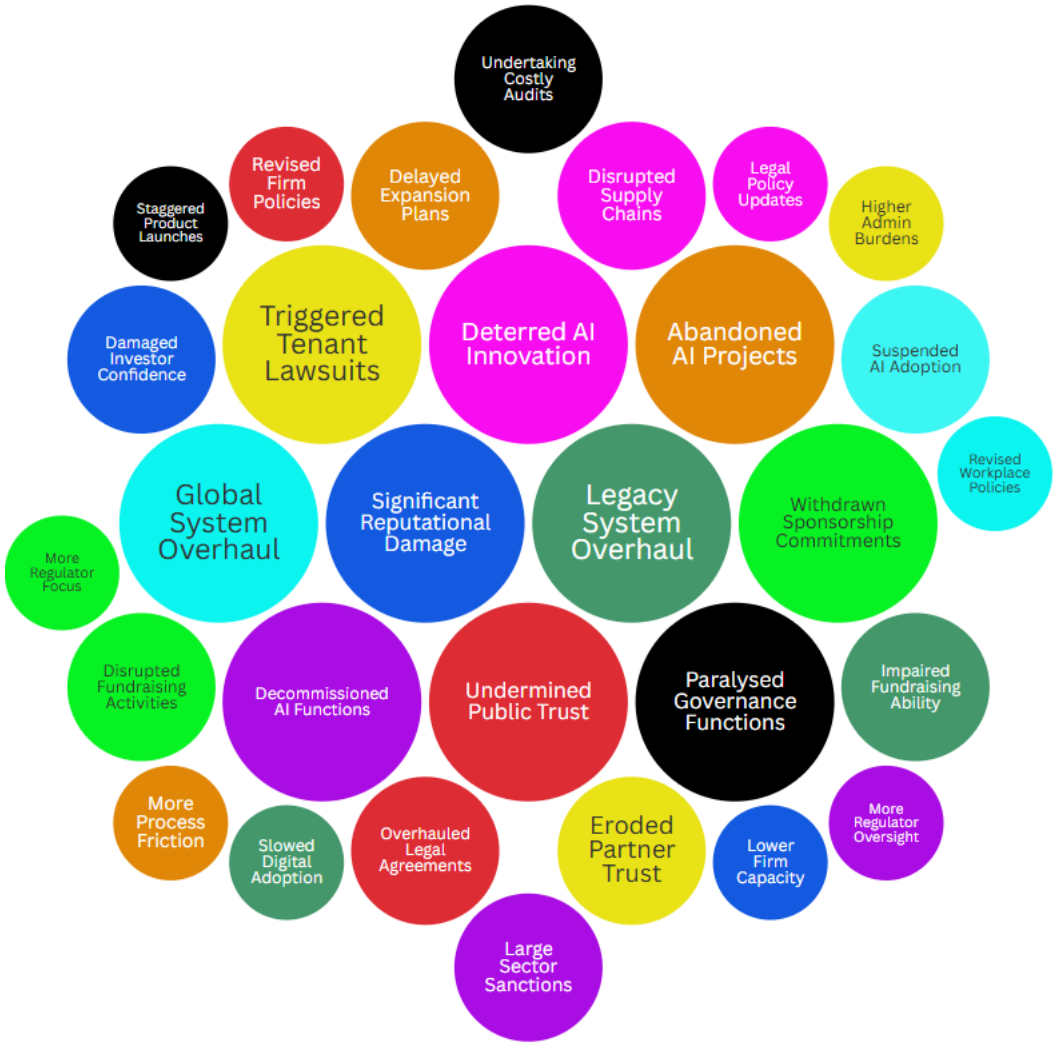
EU AI Act enforcement will likely arise in high-risk sectors such as finance, healthcare, industry, media, public services, and employment. These areas involve sensitive personal data, automated decision-making, biometric surveillance, and large-scale AI deployment, making them primary targets for regulators focused on transparency, accountability, and consumer protection.

What mitigating measures can firms deploy?

Firms can mitigate risks by implementing privacy-by-design, conducting AI impact assessments, ensuring algorithmic transparency, and maintaining robust documentation. Regular audits, staff training, fairness testing, and clear user consent mechanisms are critical. Establishing cross-functional governance and integrating compliance from development stages will reduce exposure to penalties and reputational damage.

Assessing impact of forecasted EU AI Act fines drawn from GDPR Enforcement Data

Forecasted Impact of EU AI Act enforcement Action by Sector



Legend

- Finance, Insurance, and Consulting
- Accommodation & Hospitality
- Health Care
- Industry & Commerce
- Real Estate
- Media, Telecoms & Broadcasting
- Public Sector & Education
- Transportation & Energy
- Individuals & Private Associations
- Employment

GDPR Enforcement Action		EU AI Act Impact (Size)		
Section	Description	Small	Medium	Large
Finance, Insurance, and Consulting	As of the 2024 ETR, DPAs in 24 countries issued 215 fines totalling EUR 57.3 million (+EUR 22.2M from 2023) in the finance, insurance, and consulting sectors—primarily for insufficient legal basis for data processing and inadequate security measures. Spain led in both volume (64 fines) and value, including five fines over EUR 1 million, with the highest (EUR 6M) targeting unlawful intra-group data sharing without valid consent. These cases consistently revealed failures in consent mechanisms, transparency, and technical safeguards, underscoring systemic compliance gaps. Given these trends, enforcement under the EU AI Act will likely focus on similar vulnerabilities—especially consent, transparency, data minimization, and security—in high-risk AI systems within regulated sectors.	For smaller AI providers and users in finance, insurance, and consulting, fines under the EU AI Act will likely remain proportionate to their size, targeting procedural shortcomings rather than systemic failures. While not financially devastating, these penalties will impose a heightened administrative burden, forcing firms to allocate more resources to documentation, staff training, and internal audits. The need for ongoing compliance monitoring may slow development cycles and reduce agility, particularly for startups and niche players. Repeated minor infractions could also draw increased regulatory attention, leading to more frequent inspections and reporting requirements that strain limited operational capacity.	Mid-sized firms face fines that could meaningfully impact their financial stability and strategic direction. Penalties in this tier would stem from material gaps in AI governance, such as inadequate risk mitigation or insufficient transparency in automated decision-making. The financial strain may force firms to delay or scale back AI initiatives, putting them at a competitive disadvantage. Beyond direct costs, these penalties often come with mandated corrective measures, such as third-party audits or system modifications, which divert resources from core business activities. Persistent compliance issues may also damage client and investor confidence, making it harder to secure partnerships or funding for future projects.	For major financial institutions, insurers, and consulting firms, fines under the EU AI Act could reach levels that threaten long-term profitability and market position. Violations involving high-risk AI systems, such as biased algorithms or large-scale data mismanagement, may trigger penalties severe enough to necessitate restructuring of key business units. Beyond the immediate financial hit, firms risk enforced suspension of critical AI applications, disrupting operations in areas like credit scoring or fraud detection. The reputational fallout from such penalties could lead to loss of major clients, shareholder lawsuits, and lasting brand damage. Regulators may also impose enhanced oversight requirements, subjecting firms to years of stringent compliance obligations that hinder innovation and growth.
Accommodation & Hospitality	As of the 2024 ETR, DPAs in 14 countries issued 72 fines totaling approximately EUR 22.5 million (+13 fines, +EUR 0.1M from 2023) in the accommodation and hospitality sector, with Spain alone accounting for over half (37 fines). Over 60% of these fines (46 cases) involved unlawful video surveillance—primarily due to capturing public spaces (violating data minimization) and failing to provide proper notice—highlighting persistent compliance issues. Although most penalties remain modest (83% under EUR 20,000), notable exceptions include fines against Marriott (EUR 20.45M, UK) and ACCOR SA (EUR 600,000, France). Additional violations involved unlawful collection of	Small hotels and hospitality businesses will likely face fines targeting basic AI governance failures, such as inadequate documentation of automated decision systems or minor transparency lapses. While not financially crippling, these penalties will require investment in compliance training and process adjustments. Family-run establishments using simple AI tools (like chatbots) may struggle with new regulatory requirements, potentially slowing digital adoption. Recurring violations could trigger additional reporting obligations, creating administrative burdens disproportionate to their operations.	Mid-sized hotel chains and booking platforms risk penalties for material violations like improper AI-driven surveillance or biased pricing algorithms. Fines at this level could force temporary suspension of automated systems, disrupting daily operations like check-in processes or dynamic pricing. The sector's heavy reliance on customer-facing AI makes it particularly vulnerable to reputational harm from transparency failures. Companies may need to retrofit existing surveillance infrastructure or overhaul data collection practices, incurring significant unplanned costs. Regional operators could face competitive disadvantages if compliance costs limit their ability to match larger rivals' AI investments.	Multinational hospitality groups face existential risks from AI Act violations, particularly around biometric surveillance or algorithmic discrimination in guest services. A major fine could trigger chain-wide system shutdowns, paralyzing operations across hundreds of properties. The sector's customer-centric nature amplifies reputational fallout - a single incident of AI-enabled profiling could spark widespread media coverage and consumer backlash. Legacy systems in older properties may require complete replacement to meet technical standards, necessitating capital-intensive overhauls. At this scale, violations could permanently alter brand perception in an industry where trust is paramount, with recovery potentially taking years.

	guest data without a valid legal basis. These trends suggest that under the EU AI Act, enforcement in this sector may target improper surveillance practices, lack of transparency, and excessive data collection—especially where biometric or AI-enhanced monitoring tools are deployed.			
Health Care	As of the 2024 ETR, DPAs in 26 countries issued 202 fines totaling EUR 16.5 million for GDPR violations in the healthcare sector—a 20% drop in fines and over 70% drop in total fine value compared to 2023, continuing the trend toward lower average penalties. Most fines (71) stemmed from insufficient technical and organizational measures (TOMs), especially related to cybersecurity failures such as ransomware attacks and unauthorized access to patient data. The largest fine in 2023 (EUR 460,000, Ireland) involved poor breach response and data loss affecting 70,000 individuals. Italy remained the most active DPA, while new enforcers like Lithuania entered the landscape. Additional cases involved denial of access rights and outdated legal bases for processing, including COVID-era data use. These enforcement patterns suggest the EU AI Act may similarly prioritize cybersecurity resilience, lifecycle compliance for data processing, and the enforceability of rights—especially as AI adoption accelerates in sensitive healthcare contexts.	Small healthcare providers and clinics using limited AI tools (e.g., diagnostic support or appointment scheduling) will likely face fines for procedural gaps, such as inadequate documentation of AI decision-making or minor transparency lapses. While not financially severe, these penalties will necessitate updates to patient consent processes, staff training, and record-keeping systems. Solo practitioners and small practices may struggle with compliance overhead, potentially delaying AI adoption. Recurring violations could trigger additional audits, creating administrative burdens that divert attention from patient care.	Mid-sized hospitals and telehealth platforms risk penalties for material failures in AI governance, such as insufficient cybersecurity protections for patient data processed by AI or biased algorithmic outputs in treatment recommendations. Fines at this level could force temporary suspension of AI-driven diagnostics or analytics tools, disrupting clinical workflows. The sector's sensitivity to patient trust means even moderate penalties may erode confidence among patients and partners. Organizations may need to retrofit IT infrastructure or overhaul data-sharing agreements, incurring unplanned costs and operational delays. Regional healthcare networks could face competitive disadvantages if compliance complexities slow their ability to integrate advanced AI solutions.	Major hospital chains, pharmaceutical firms, and national health systems face severe penalties for high-risk AI violations, such as unsafe patient triage algorithms or large-scale breaches of sensitive health data. A major fine could mandate shutdowns of critical AI systems, paralyzing operations in areas like medical imaging analysis or drug discovery. Given healthcare's zero-tolerance for errors, violations may trigger lawsuits, regulatory investigations, and lasting reputational damage—particularly if patient harm is alleged. Legacy EHR systems may require costly replacements to meet AI Act standards. At this scale, non-compliance could undermine public trust in digital health initiatives and deter future AI investment in the sector.
Industry & Commerce	As of the 2024 ETR, DPAs in 26 countries have issued 455 fines totaling EUR 897 million (+83 fines, +EUR 40M from 2023) in the industry and commerce	Small and medium-sized manufacturers, retailers, and commercial service providers will likely face fines for procedural shortcomings in AI deployment, such as inadequate documentation	Mid-sized industrial firms and e-commerce platforms risk penalties for material AI governance failures, such as non-transparent algorithmic pricing, unlawful employee monitoring, or inadequate	Multinational manufacturers, tech conglomerates, and global retailers face existential risks from AI Act violations, particularly in areas like mass surveillance, discriminatory algorithms, or unethical data

	sector, making it the most frequently sanctioned and second most heavily fined sector under the GDPR. The Amazon group alone accounts for over 85% of the total fine volume, including a EUR 32 million fine (2023, France) for unlawful employee surveillance and a record EUR 746 million fine (2021, Luxembourg). Most fines cite insufficient legal basis for processing (109 cases), inadequate information provision (96), and general GDPR principle violations (80). CNIL's ongoing action against Clearview AI underscores the risk of compounded sanctions for non-compliance post-enforcement. These trends suggest that under the EU AI Act, enforcement in this sector may focus on transparency, lawful processing of personal data—including biometric—and the responsible use of AI in employee monitoring and large-scale data collection.	of automated decision-making processes or insufficient employee training on AI systems. While not financially debilitating, these penalties will require updates to internal governance frameworks, including revised data collection policies and transparency measures. Smaller businesses may experience operational friction as they implement compliance protocols, potentially delaying AI adoption or digital transformation initiatives. Recurring minor violations could trigger additional regulatory scrutiny, increasing administrative burdens for compliance teams.	safeguards for customer data processed by AI systems. Fines at this level could necessitate temporary suspension of AI-driven logistics, inventory management, or customer profiling tools—disrupting supply chains and sales operations. The sector's reliance on data-intensive processes means compliance failures may also erode business partner trust and trigger contractual repercussions. Companies may face unplanned costs to audit and retrofit AI systems, particularly in legacy manufacturing or retail environments where technical debt complicates compliance.	scraping practices. Severe penalties could force shutdowns of core AI systems used in workforce management, personalized marketing, or industrial automation—paralyzing operations across international networks. Given the sector's visibility, violations may spark consumer boycotts, investor backlash, and multidaytional lawsuits, especially if AI misuse affects labor rights or consumer fairness. Legacy systems in factories or retail networks may require prohibitively expensive overhauls to meet technical standards. At this scale, non-compliance could redefine market positions and deter AI innovation for years.
Real Estate	As of the 2024 ETR, 63 fines have been imposed on data controllers in the Real Estate sector, totaling slightly over EUR 2.6 million (+10 fines, +EUR 20,000 from 2023). Although the total amount remains low compared to other sectors, notable fines include EUR 1.9 million (Germany, Bremen) for unlawful data processing and EUR 400,000 (France, CNIL) for excessive data storage and lack of security. Around 40% of fines result from non-compliance with general data processing principles, and over 30% from insufficient legal basis for data processing. Video surveillance remains a key issue, with fines arising from inadequate information provision, unnecessary data	Small real estate agencies and independent property managers will likely face fines for minor AI-related compliance gaps, such as inadequate documentation of automated tenant screening processes or insufficient transparency in AI-powered valuation tools. While not financially severe, these penalties will require updates to data handling procedures, client disclosure protocols, and staff training—creating administrative burdens for lean operations. Recurring violations could trigger additional reporting requirements, potentially slowing transaction workflows. The sector's fragmentation means many small players may initially struggle with AI governance basics, though the impact will primarily involve process refinements rather than existential threats.	Mid-sized property tech firms and regional developers risk penalties for material AI failures, such as biased algorithmic pricing models, unlawful tenant profiling, or insecure smart building data collection. Fines at this level could force temporary suspension of AI-driven tools for market analysis or automated viewings, disrupting sales pipelines. The sector's increasing reliance on proptech solutions means compliance failures may erode partner trust and delay funding rounds. Firms may incur unplanned costs to audit AI systems, particularly where legacy property management software integrates poorly with new transparency requirements. Reputational harm from discriminatory algorithm claims could be especially damaging in this relationship-driven industry.	Major real estate investment trusts (REITs), global proptech platforms, and smart city developers face severe penalties for systemic AI misuse—particularly in automated surveillance (e.g., facial recognition in residential complexes) or large-scale tenant data exploitation. A major fine could mandate shutdowns of AI-powered security or dynamic pricing systems, paralyzing operations across property portfolios. Given growing public sensitivity to housing equity, violations may trigger tenant lawsuits, local government sanctions, and lasting brand damage—especially if AI systems exacerbate housing discrimination. Retrofitting smart buildings for compliance could prove prohibitively expensive, while institutional investors may divest from firms with recurring AI governance failures.

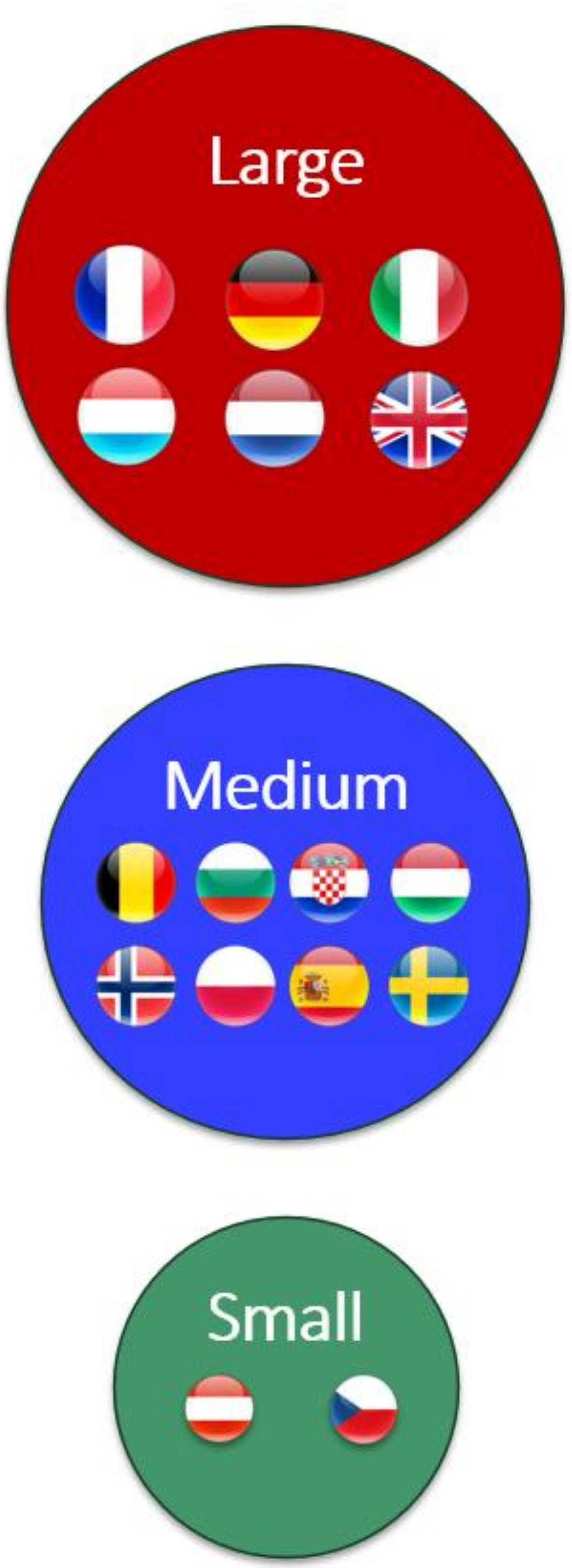
	capture, and improper placement of cameras. These trends suggest that under the EU AI Act, enforcement in this sector may focus on data minimization, transparency, and security measures in surveillance systems, particularly where AI-driven monitoring tools are used.			
Media, Telecoms & Broadcasting	As of 2024, the media, telecommunications, and broadcasting sector has accumulated EUR 3.3 billion in fines from 288 cases across 21 countries, marking an increase of EUR 1.6 billion and 70 more fines compared to 2023. This sector represents nearly 75% of all fines imposed across all industries, largely due to high-turnover companies. In 2023, Meta faced a record fine of EUR 1.2 billion for violating international data transfer rules, following the ECJ's "Schrems II" ruling on US data protection. TikTok received significant fines for mishandling children's data, including EUR 345 million from the Irish DPC and EUR 14.5 million from the UK ICO. The French CNIL also imposed a EUR 40 million fine on Criteo for improper user consent in personalized advertising. Fines in this sector have increased by 94%, with violations mainly related to insufficient legal basis for data processing and non-compliance with general data protection principles. Meta's record fine underscores the role of the European Data Protection Board's dispute resolution procedures in shaping GDPR enforcement, particularly in Ireland.	Smaller media outlets, local telecom providers, and independent broadcasters will likely face fines for procedural AI compliance gaps, such as inadequate documentation of algorithmic content moderation or insufficient transparency in targeted advertising systems. While not financially devastating, these penalties will necessitate updates to user consent flows, data governance policies, and staff training—creating operational friction for resource-constrained organizations. Niche streaming platforms or regional news aggregators may need to limit AI-driven personalization features to avoid compliance risks, potentially reducing audience engagement. Recurring violations could trigger additional supervisory measures, increasing the administrative burden for lean operations.	Mid-sized streaming services, ad-tech firms, and telecom operators risk penalties for material AI violations, such as biased content recommendation algorithms, unlawful voice-data processing, or insufficient protections for minors' data in AI systems. Fines at this level could force temporary suspension of personalized advertising or viewer profiling tools, disrupting revenue streams. The sector's reliance on user data monetization means compliance failures may scare away advertising partners or delay expansion plans. Firms may face costly overhauls of legacy recommendation engines or voice-assistant technologies to meet transparency requirements. Reputational damage from AI-related privacy scandals could be particularly harmful for brands building trust in competitive markets.	Global social media platforms, telecom conglomerates, and streaming giants face unprecedented risks under the AI Act—especially around mass data processing, deepfake proliferation, or manipulative algorithmic design. Potential fines reaching billions could mandate fundamental restructuring of core business models (e.g., meta's ad-targeting infrastructure). Violations may trigger service limitations in key markets, as seen with TikTok's regional bans. The sector's public visibility means AI governance failures often spark user backlash, advertiser revolts, and regulatory chain reactions across jurisdictions. Compliance may require abandoning lucrative but high-risk AI practices altogether, with lasting impacts on profitability. For dominant players, enforcement could redefine the entire digital media landscape.
Public Sector & Education	As of 2024, DPAs from 25 countries have imposed 243 fines on public and education sector entities, totaling over EUR 27.5 million, reflecting a EUR 3.4	Municipal offices, small schools, and local public services will likely face fines for procedural gaps in AI deployment, such as inadequate documentation of automated decision-	Mid-sized universities, regional government agencies, and public healthcare providers risk penalties for material AI failures, such as biased algorithmic eligibility	Federal agencies, national education ministries, and major research institutions face severe penalties for systemic AI misuse—especially in mass surveillance, predictive policing, or discriminatory

	million increase from 2023. The majority of fines are related to insufficient legal bases for data processing (83 fines) and inadequate technical and organizational measures (68 fines), with a rising number of cases concerning non-compliance with general data protection principles (47 fines). Key trends include an uptick in fines related to the use of digital tools in education, such as online learning platforms and video conferencing, along with the processing of sensitive data, particularly health data during the COVID-19 pandemic. Notable cases include the Italian DPA's fines against the Veneto Region for disclosing vaccination status data (EUR 100,000) and the city of Rome for disclosing abortion-related data (EUR 176,000). The highest fine in the sector was EUR 4.3 million against the Portuguese National Statistical Institute for violations related to the 2021 census, and the Dutch Tax and Customs Administration received a EUR 3.7 million fine for unlawful data processing in a fraud risk list. The public and education sectors face growing scrutiny, especially regarding sensitive data processing and digital technology use, with a continued focus on maintaining high data protection standards, particularly for minors.	making in student admissions or insufficient transparency in citizen-facing chatbots. While not financially crippling, these penalties will require updates to data governance frameworks, staff training, and public disclosure protocols—straining limited administrative resources. Small educational institutions using basic AI tools (e.g., plagiarism detection or learning analytics) may need to simplify or pause certain features to ensure compliance. Recurring violations could trigger additional oversight, diverting attention from core public service delivery.	assessments (e.g., for social benefits) or insecure processing of student/sensitive citizen data. Fines at this level could force temporary suspension of AI-driven systems for welfare distribution, exam proctoring, or public record management—delivering critical services. The public sector's budget constraints mean compliance costs may reduce funding for other digital transformation projects. Persistent violations could erode public trust in government technology initiatives, particularly where AI systems affect vulnerable populations. Organizations may face costly audits and mandatory third-party certifications for high-risk AI applications.	automated decision-making in public services. A major fine could mandate nationwide suspension of AI tools used in immigration control, tax fraud detection, or standardized testing—paralyzing core government functions. Given the sector's duty of care, violations involving minors' data (e.g., through educational AI) may trigger political scandals and legislative backlash. Retrofitting legacy public sector IT systems for AI compliance could require years and billions in public funds. At this scale, enforcement actions may redefine the boundaries of state AI use for a generation.
Transportation & Energy	In 2024, DPAs from 20 countries imposed 109 fines in the transportation and energy sector, totaling around EUR 105 million, marking a EUR 20 million increase compared to 2023. While the number of fines grew, the average fine slightly decreased to EUR 796,000. Common reasons for fines	Small transport operators and regional energy providers will likely face fines for technical compliance gaps, such as inadequate documentation of AI-driven logistics systems or insufficient transparency in smart meter data collection. While not financially devastating, these penalties will require updates to data governance policies, employee training programs,	National rail operators, mid-sized energy distributors, and logistics platforms risk penalties for material AI failures, such as flawed algorithmic routing systems, improper processing of customer mobility data, or insecure smart grid management. Fines at this level could force temporary suspension of AI-powered dynamic pricing, predictive maintenance, or automated	Global shipping conglomerates, international airlines, and major energy producers face existential risks from AI Act violations—particularly in mass surveillance (e.g., facial recognition at airports), discriminatory algorithmic pricing, or unsafe autonomous transport systems. Severe penalties could mandate shutdowns of AI-driven traffic management, smart grid

	included insufficient legal basis for data processing and inadequate technical and organizational measures. Notable cases include a EUR 1 million fine against Autostrade per l'Italia S.p.A. for mishandling data in its toll reimbursement app, a EUR 10 million fine against Axpo Italia S.p.A. for activating contracts without consent based on inaccurate data, and a EUR 6.1 million fine on ENDESA ENERGÍA S.A.U. for a security breach. The trend of rising fines in this sector highlights the need for companies to prioritize compliance, especially regarding data handling and security measures.	and system audit procedures—creating operational friction for organizations with limited IT resources. Municipal transit authorities or local utility companies may need to simplify or delay AI adoption in areas like demand forecasting or automated billing due to compliance complexities. Recurring violations could trigger additional regulatory oversight, potentially affecting service expansion plans.	dispatch systems—disrupting core operations. The sector's critical infrastructure status means compliance failures may also trigger sector-specific sanctions from transport/energy regulators beyond GDPR-style fines. Companies may face unplanned costs to upgrade IoT device security or retrofit legacy systems, with potential knock-on effects on consumer pricing.	controls, or cargo logistics networks—potentially paralyzing cross-border operations. Given the sector's safety-critical nature, violations may trigger cascading sanctions from aviation, maritime, and energy authorities alongside EU fines. Retrofitting infrastructure like smart charging networks or autonomous vehicle systems for compliance could require billions in investment. At this scale, enforcement could reshape entire business models in mobility-as-a-service and energy trading.
Individuals & Private Associations	In 2024, DPAs from 17 countries imposed 308 fines in the individuals and private associations sector, totaling EUR 1.85 million, a modest increase from the previous year. The highest fine of EUR 525,000 was issued to the Royal Dutch Tennis Association for unlawfully selling member contact details to sponsors for direct marketing. Fines over EUR 20,000 were mainly imposed on large non-profits, particularly sports associations, for violations like insufficient data protection measures. Private individuals received smaller fines, often under EUR 2,000, with many cases involving illegal video surveillance. The Spanish DPA imposed the majority of fines in this sector, highlighting a continued focus on video surveillance and strict compliance requirements for both individuals and organizations.	Private individuals and small community associations will likely face minor fines for isolated AI-related violations, such as improper use of facial recognition in home security systems or non-compliant data collection in neighborhood apps. These penalties will primarily serve as warnings, requiring corrective measures like system adjustments or privacy notices rather than imposing severe financial hardship. However, recurring violations could lead to escalated scrutiny, particularly for persistent offenders using AI-powered surveillance tools. The administrative burden of compliance may discourage casual adoption of consumer-grade AI technologies in private settings.	National sports federations, large membership organizations, and event organizers risk meaningful penalties for systemic AI misuse—such as unauthorized biometric profiling of participants or algorithmic discrimination in membership processing. Fines at this level could force temporary suspension of AI-driven marketing systems or member analytics platforms, disrupting fundraising and engagement activities. Non-profits may struggle with compliance costs for auditing AI tools used in donor profiling or event security. Reputational damage from data misuse scandals could be particularly damaging for organizations reliant on public trust and participation.	Major international associations and data-driven philanthropic organizations face severe consequences for large-scale AI violations—especially involving sensitive member data exploitation or cross-border data transfers. Penalties could reach percentages of global donation income, potentially crippling operations for organizations already working with limited margins. Systemic failures in consent mechanisms (like the tennis association case) might trigger class-action lawsuits from members alongside regulatory fines. At this scale, violations could lead to sponsorship withdrawals and lasting membership declines, fundamentally threatening organizational viability.
Employment	In 2024, DPAs imposed 135 fines related to employee data processing, totaling over EUR 59 million, marking a significant increase	Small and medium-sized employers will likely face fines for procedural gaps in AI-driven HR tools, such as inadequate transparency in automated resume screening	Corporate employers and staffing platforms risk penalties for material AI failures in workforce management, such as discriminatory algorithmic	Global enterprises and gig economy platforms face existential threats from systemic AI violations—particularly in mass employee surveillance, predictive

	from the previous year. The average fine remained stable at EUR 500,000. The highest fine was EUR 10 million, issued by the Dutch DPA for a mobility service provider's failure to provide adequate information about data storage and employee access to their data. Many fines were based on improper storage of sensitive employee data or failure to meet information obligations, with some related to specific employment law issues. Employee data processing continues to be a primary focus for DPAs, driven by data subject complaints, particularly in termination scenarios. Employers are urged to ensure compliance, as employee data protection remains integral to both legal proceedings and labor disputes.	or insufficient documentation of employee monitoring systems. While not financially devastating, these penalties will require updates to workplace policies, staff training, and employee notification procedures—creating administrative burdens for HR departments. Recurring violations could trigger labor inspections or complicate dismissal proceedings. Small businesses using basic AI scheduling or productivity tools may need to limit functionality to ensure compliance, potentially reducing operational efficiency.	hiring tools, unlawful employee monitoring (e.g., keystroke logging), or insecure processing of sensitive HR data. Fines at this level could force suspension of automated recruitment systems or workforce analytics platforms, disrupting hiring and performance management. The potential for employee lawsuits alongside regulatory action creates compounded liability risks. Companies may face costly audits of HR tech stacks and mandatory revisions to collective bargaining agreements where AI systems affect worker rights. Reputational damage could impact talent acquisition in competitive job markets.	termination algorithms, or cross-border HR data transfers. Severe penalties could mandate shutdowns of entire workforce management systems, paralyzing operations across jurisdictions. Given rising worker activism, violations may trigger union actions, class-action lawsuits, and multi-country enforcement proceedings. The Dutch mobility service case (€10M fine) demonstrates how employee data rights violations can attract maximum-tier penalties. At this scale, compliance failures could necessitate complete overhauls of global HR infrastructures and permanently alter employer-employee power dynamics.

Forecasted Impact of EU AI Act Enforcement Action by Country



GDPR		EU AI Act
Country	Description	Impact
Austria	Limited transparency exists in Austria regarding the publication of fines, with the Austrian Data Protection Authority (DPA) referring to European Data Protection Board (EDPB) guidelines for fine calculations. Class actions by consumer protection associations, such as the "Verein für Konsumenteninformation" (VKI), are permitted and encouraged under the GDPR. While fines generally outweigh damages in Austria, the number of lawsuits before civil courts is growing, a trend expected to continue due to clearer European Court of Justice (ECJ) rulings on damages. Public authorities cannot be fined. The DPA has focused its audits on sectors such as finance, particularly regarding marketing data usage, legal bases for processing, and data transfers. A notable fine of EUR 20,000 was imposed for unlawful employee surveillance, and another significant case involved an EUR 18 million fine on the Austrian Postal Service, which was appealed and remains under review. The DPA is a federal authority with about 60 employees and an annual budget of EUR 4.7 million, operating under the Ministry of Justice. Fines are imposed through administrative criminal proceedings, with appeals going through the Austrian Federal Administrative Court and potentially the Constitutional Court or Austrian Supreme Administrative Court. Fines are paid into the federal treasury, and while no official fine calculation method is publicly available, the DPA follows internal guidelines aligned with the EDPB's, considering factors like aggravating and mitigating circumstances. Public authorities are exempt from fines under the Austrian Data Protection Act. The DPA does not publish all fines but shares anonymized decisions and trends through its newsletter and annual reports. Consumer protection associations can file cases on behalf of consumers, and while Austria does not permit class actions, the ECJ has supported the right for associations to litigate data protection cases. The trend of fines surpassing civil damages continues, though lawsuits are expected to rise as the ECJ's decisions on damages and data protection law gain traction.	Austria is likely to see a medium-scale impact from enforcement fines under the EU AI Act, mirroring patterns observed under the GDPR. While the Austrian DPA operates with limited transparency and modest resources, its adherence to EDPB guidelines, focus on high-risk sectors, and history of issuing significant fines—such as the EUR 18 million case—suggest a capacity for impactful enforcement. The growing trend of civil litigation and involvement of consumer protection associations further supports this. However, exemptions for public authorities and selective publication of fines may temper overall visibility and deterrence, keeping Austria's enforcement impact below the EU's most aggressive regulators.
Bulgaria	Fines can be imposed on authorities and public entities in Bulgaria, with the highest fine to date being imposed on a public authority. Complaints addressed to the Bulgarian Commission for Personal Data Protection (CPDP) are steadily increasing, and part of the decisions issued by the CPDP are made public on its website. Fines are generally more significant than litigation in addressing alleged violations, with changes to this trend unlikely due to the high costs and lengthy nature of legal proceedings. The CPDP primarily initiates proceedings based on complaints from data subjects, and although it does not focus deliberately on specific types of violations, most fines have been related to violations of personal data processing principles, insufficient legal bases for processing, inadequate security measures, and failure to comply with data	Bulgaria is expected to experience a medium-to-large impact from enforcement fines under the EU AI Act, based on its GDPR enforcement record. The Bulgarian CPDP has demonstrated a willingness to impose substantial fines, including on public authorities, with the highest reaching EUR 2.55 million. The authority acts primarily on complaints and covers a broad range of sectors, showing readiness to address systemic issues. Although class actions are rare, the CPDP's independence, steady complaint volume, and transparency in publishing enforcement outcomes suggest strong institutional capacity. Given this context, AI Act fines are likely to follow a similar path,

	subjects' rights requests. Common sectors for complaints include video surveillance, banking, state affairs, employment relations, and telecommunications. The largest fine imposed in Bulgaria was approximately EUR 2,550,000 on the Bulgarian National Revenue Agency (NRA) in 2019 for failing to implement adequate data protection measures, leading to the unauthorized access and dissemination of personal data. Although the NRA appealed the decision, the case was dismissed due to the statute of limitations. The issue has been referred to the Court of Justice of the European Union (CJEU) for further clarification on liability in cases involving criminal activity. The CPDP is an independent authority with 117 staff members, a 2023 budget of approximately EUR 3.5 million, and is organized into four directorates. Fines are imposed as part of administrative proceedings, and companies can appeal decisions within 14 days. The proceeds from fines are credited to the CPDP's budget. There is no publicly available standard fine calculation methodology, but the CPDP follows guidelines from the Art. 29 Working Party. Public authorities can also be fined, with the proceeds going to the CPDP’s budget. The CPDP publishes information on fines and procedural steps on its website and in its annual reports, though the identities of affected companies are generally not disclosed unless the case is of public interest. In 2023, the CPDP received 925 complaints, a slight increase from the previous year, and imposed fines totaling approximately EUR 46,500. Bulgaria allows class actions under the Civil Procedure Code, though these are rare in data protection cases, and most claims for compensation are pursued individually. The trend in Bulgaria indicates that fines from authorities will continue to outweigh court proceedings, with the CPDP's role in enforcing the GDPR remaining crucial.	
Belgium	As of 2024, Belgium's data protection authority (DPA) has focused on sectors such as telecommunications, media, government, direct marketing, education, and SMEs, with priorities including cookies, DPOs, smart cities, and data brokers. The most significant fine to date was EUR 600,000 against Google Belgium for not respecting the right to be forgotten, though it was annulled by the Court of Appeal, which ruled that Google Belgium was not the appropriate entity for corrective measures. The DPA follows a transparent approach to publishing fines, with involved parties often anonymised. The fine procedure involves complaints or self-initiated investigations, followed by proceedings before the Litigation Chamber, with appeals possible within 30 days to the Market Court. Fines are transferred to the state treasury, and while Belgium allows class actions for data protection claims, high litigation costs and low damages claims mean that fines currently play a more prominent role. The DPA plans to continue its proactive approach, with an increasing number of decisions, though the total amount of fines remains lower than in neighboring countries.	Belgium is likely to see a medium-scale impact from enforcement fines under the EU AI Act, reflecting its balanced but cautious approach under the GDPR. The Belgian DPA has prioritized diverse sectors and proactively launched investigations, though total fines remain modest compared to other EU countries. Its most notable fine—EUR 600,000 against Google Belgium—was annulled, highlighting procedural constraints that may temper enforcement. Nonetheless, the DPA’s structured litigation process, transparency, and focus on high-risk areas such as smart cities and data brokers indicate readiness to enforce the AI Act. While class actions exist, fines are expected to remain the primary enforcement tool.
Croatia	In Croatia, the Data Protection Agency (AZOP) independently enforces GDPR compliance and can	Croatia is poised for a medium-to-large impact from EU AI Act enforcement fines, reflecting its

	impose fines through formal decisions, which may be challenged in administrative court. Enforcement activity has significantly increased, with 90% of total fines issued in 2023, though public authorities cannot be fined. Fines are generally published on the Agency's website in anonymized form unless they meet criteria for full disclosure, such as high value or repeat violations. While class actions are possible under broader civil or consumer laws, they must be initiated by authorized entities. Fines are more impactful than damages due to their reputational consequences. Historically, the Agency has focused on sectors like media, social networks, marketing, retail, gambling, and notably debt collection in 2023. Common violations include unlawful processing, inadequate technical safeguards, data leaks, and improper surveillance. For 2024, planned inspections will emphasize the social security, health, banking, tourism, insurance, and gambling sectors. The largest fine to date—EUR 5.47 million—was issued to a debt collection agency for processing sensitive data without legal basis, poor security, and lack of transparency; it is likely under appeal. The Agency, staffed by 35 people and funded through the state budget, conducts both announced and unannounced inspections and may seal or seize evidence during investigations. Fines are paid into the state treasury and there is no standardized fine calculation model; instead, various aggravating and mitigating factors are considered. Annual reports provide aggregated data on enforcement, with a sharp rise in cases and sanctions in recent years, indicating a growing regulatory role in shaping compliance.	sharply rising GDPR activity. With 90% of total fines issued in 2023 alone and a record EUR 5.47 million fine for unlawful data processing, the Croatian DPA (AZOP) has demonstrated increasing assertiveness. Although public authorities are exempt from fines, AZOP's expanding focus on high-risk sectors—like health, banking, and insurance—positions it well for AI oversight. Its ability to conduct unannounced inspections and impose significant penalties enhances deterrence. Given its growing enforcement footprint, Croatia is expected to apply the AI Act with escalating financial and reputational consequences.
Czech Republic	In the Czech Republic, fines for data protection violations are comparatively low, with the highest recorded fine being around EUR 300,000 for unsolicited commercial communications. Fines are imposed by the Úřad pro ochranu osobních údajů (UOOU), which conducts thorough audits, primarily focusing on issues like inadequate legal bases for data processing and data security deficiencies. The UOOU's control plan for 2024 will focus on personal data processing by public authorities and companies in sectors like delivery services and telecommunications. Fines cannot be imposed on public authorities, and although fines are paid into the state budget, the UOOU does not have an official calculation methodology for fines, instead relying on factors like the severity of the breach and the number of affected data subjects. Private litigation for data breaches is uncommon in the Czech Republic due to high litigation costs and low damage claims, making administrative fines more prominent. The UOOU does publish some case information, but typically with redactions, and only aggregated data is available through official requests.	The Czech Republic is likely to experience a small-to-medium impact from enforcement fines under the EU AI Act, given its relatively conservative GDPR enforcement record. The UOOU has issued modest fines to date, with the highest around EUR 300,000, and focuses on audits rather than large-scale punitive actions. Public authorities are exempt from fines, and the lack of a standardized calculation method may limit consistency or escalation in enforcement. While the UOOU actively monitors sectors like telecom and delivery, limited transparency and rare private litigation suggest a restrained enforcement culture. AI Act fines may rise modestly but are unlikely to be severe.
France	The French Data Protection Authority (CNIL) primarily focuses on enforcing GDPR compliance through fines, with an emphasis on legal bases for data processing, security requirements, and sector-specific issues. The CNIL does not impose fines on public authorities, but it may take enforcement actions against them. Fines are relatively high, with the largest imposed on	France is expected to experience a large-scale impact from enforcement fines under the EU AI Act, based on its assertive GDPR enforcement record. The CNIL has imposed some of the highest fines in Europe—up to EUR 150 million—and demonstrates strong institutional capacity with significant staffing

	Google for EUR 150 million in 2021. The CNIL operates independently with an annual budget of EUR 21.8 million and 245 staff members. While fines are more common than court proceedings for damages, class actions can be filed by certain associations. The CNIL's procedures allow companies to appeal decisions within two months, and fine proceeds go to the state treasury. Its annual report aggregates enforcement data, providing transparency on investigations and penalties.	and budget. Its proactive approach, clear focus on high-risk issues like legal basis and security, and robust transparency practices position it as a leading enforcer. Although public authorities are exempt from fines, CNIL can still take enforcement actions against them. With class actions also permitted, France is likely to maintain a prominent role in AI Act enforcement.
Germany	Germany's data protection enforcement is shaped by 16 regional authorities and the Federal Commissioner for Data Protection (BfDI). Fines often stem from issues with legal bases for data processing or security deficiencies, particularly in sectors like health, finance, and employee data. The largest fine to date was EUR 35.26 million against H&M for unlawful employee data handling. Fines are imposed through administrative procedures, with appeal options to criminal courts, and are directed to the state or federal treasury. While German DPAs are not required to publish every fine, significant cases are highlighted in reports. Germany has introduced collective redress mechanisms, such as the model declaratory action and the new collective action for redress, allowing consumer organizations to pursue claims on behalf of groups. Fines are currently more common than private litigation, but the rise of collective actions may shift the trend towards more legal disputes.	Germany is likely to face a large-scale impact from EU AI Act enforcement fines, reflecting its decentralized but assertive GDPR enforcement structure. With 16 regional authorities and the federal BfDI, Germany applies thorough scrutiny, particularly in sensitive sectors like health, finance, and employment. The country has already issued major fines—such as EUR 35.26 million against H&M—and has introduced robust collective redress mechanisms, enabling broader accountability. Although not all fines are published, significant cases are made public, reinforcing transparency. As collective legal actions grow and administrative enforcement remains strong, Germany is expected to be a key jurisdiction for impactful AI Act penalties.
Hungary	In Hungary, fines can be imposed on public authorities, albeit at reduced amounts. GDPR fines tend to be relatively low, with the largest fine to date being approximately EUR 653,000 against Budapest Bank for unlawful AI-based analysis of customer calls. While Hungarian data protection authorities (NAIH) have clear criteria for publishing fines, the focus has largely been on non-compliance issues such as improper legal bases, transparency, and data security, particularly in sectors like banking, healthcare, and telecommunications. Fines are more prominent than private litigation, as court proceedings for GDPR violations are infrequent due to high costs and lack of judicial practice. The NAIH plays a central role in enforcing data protection, with a budget of EUR 4.25 million and over 120 staff members. Fines collected are directed to the central government budget, and the NAIH has significant discretion in publishing cases, often anonymizing details. There are no model declaratory proceedings or class actions in Hungarian data protection law, and the trend points toward continued reliance on fines rather than court proceedings.	Hungary is expected to see a medium-scale impact from enforcement fines under the EU AI Act, building on its established reliance on administrative penalties over litigation. While fines under the GDPR have generally been modest, the notable EUR 653,000 fine for unlawful AI use indicates that the NAIH is prepared to act on AI-related risks. The authority’s strong focus on sectors like banking and telecommunications, combined with its discretion in publicizing fines and ability to sanction public authorities (albeit at reduced levels), suggests steady but controlled enforcement. With limited court activity and no class actions, fines will remain the primary enforcement tool.
Italy	The Italian Data Protection Authority (DPA) focuses on data protection enforcement, with fines contributing to its budget for awareness, inspections, and GDPR implementation. It has prioritized sectors like telecommunications and energy, particularly for issues such as telemarketing, unsolicited contracts, and biometric data use. Notable fines include Enel Energia's EUR 79.1 million for failing to prevent unlawful telemarketing and TIM SpA's EUR 27.8	Italy is expected to experience a large-scale impact from enforcement fines under the EU AI Act, reflecting its assertive GDPR enforcement history. The Italian DPA has issued some of Europe’s highest fines—up to EUR 79.1 million—and targets high-risk sectors like telecommunications, energy, and biometric data use. Its ability to retain part of the fines for enforcement activities creates

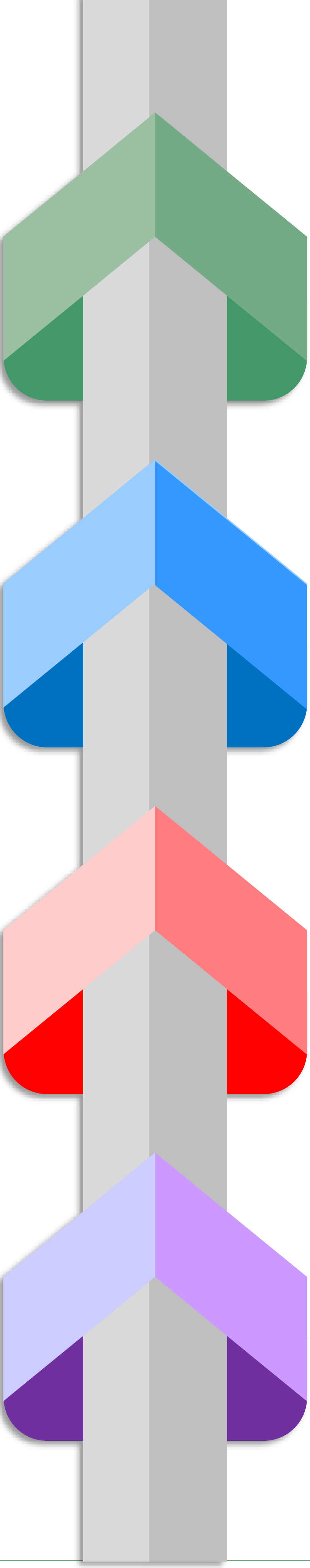
	million for improper data processing in marketing. The DPA can impose fines directly, which are split between the state treasury and its own budget. Fines are published with identifiable companies, and while fines are currently more significant than litigation, claims for damages are expected to rise, particularly in cases involving the right to be forgotten and unauthorized publication of personal images. Class actions for data protection violations are becoming more prominent, with broader access under new legislation.	strong institutional incentives for active oversight. With increasing transparency, high public visibility of fines, and growing access to class actions under new laws, Italy is well-positioned to apply the AI Act forcefully, using fines as a central mechanism for ensuring compliance.
Luxembourg	As of 2024, the Luxembourg data protection authority (CNPD) has primarily focused its investigations on the appointment of Data Protection Officers (DPOs), video surveillance systems, and vehicle tracking. In 2021, the CNPD imposed a EUR 746 million fine on Amazon for processing user data without consent, which Amazon has challenged in court, and the case is still pending. The CNPD's 2022 budget increased by 15.06% to EUR 8.2 million, and the authority employed 58 people. While the CNPD can impose fines directly, it follows a procedure where companies are notified of investigations, given the opportunity to submit observations, and can appeal fines within three months. Fines are deposited into the state treasury, and the CNPD publishes decisions, though parties are often anonymized. Luxembourg does not have a framework for class actions but is considering a bill to introduce consumer class action laws. Fines from the CNPD are currently more common than court cases, with a trend expected to continue as the authority strengthens its enforcement of GDPR compliance.	Luxembourg is likely to face a large-scale impact from enforcement fines under the EU AI Act, based on its precedent-setting GDPR enforcement. The CNPD’s EUR 746 million fine against Amazon—Europe’s largest to date—signals its capacity and willingness to impose substantial penalties, particularly for high-profile data processing violations. While the absence of a current class action framework limits private litigation, the CNPD’s structured enforcement process, growing budget, and increased staffing indicate a strengthening regulatory posture. As Luxembourg considers consumer class action legislation and continues prioritizing direct enforcement, AI Act fines are expected to play a dominant role in shaping compliance.
Netherlands	In the Netherlands, the Data Protection Authority (DPA) can impose fines on authorities and public entities, with all fines being publicly disclosed, except in two cases where anonymization is applied. Currently, fines are more significant than damages, though civil class actions for damages are expected to rise, particularly as new legislation facilitates claims. The DPA focuses on areas like AI, Big Tech, data trading, and cookie banner misuse, with most fines related to information security and non-compliance with GDPR principles. A notable fine was imposed on Uber for several transparency violations, totaling EUR 10 million, which Uber contested. The DPA operates as an autonomous body with an annual budget of EUR 40.1 million, and fines are transferred to the state treasury. While the DPA publishes detailed information on fines, including press releases and anonymized cases, the Netherlands also allows collective actions and settlements, with growing interest in class actions like the ongoing TikTok case. Fines from authorities remain more significant than court proceedings, although the number of GDPR-based civil claims is expected to rise in the coming years.	The Netherlands is positioned for a large-scale impact from EU AI Act enforcement fines, supported by its proactive and transparent data protection regime. The Dutch DPA has prioritized AI-related enforcement and already targets Big Tech, data trading, and compliance transparency, aligning closely with the AI Act’s risk-based focus. With the ability to fine public entities and a EUR 40.1 million budget, the DPA has both legal and financial capacity to pursue impactful cases. While civil class actions are gaining traction—evidenced by high-profile cases like TikTok—administrative fines remain the primary enforcement tool and are expected to remain central under the AI Act.
Norway	In Norway, the Data Protection Authority (Datatilsynet) can impose fines on authorities and public entities, with fines generally being more significant than damages due to high litigation costs and low damages awarded. Datatilsynet has focused	Norway is expected to see a medium-scale impact from EU AI Act enforcement fines, reflecting its existing enforcement approach under the GDPR. Datatilsynet has already focused on AI-related issues and demonstrated

	on areas such as children/youth, artificial intelligence, and cybersecurity, with most fines related to employee control, insufficient legal bases for data processing, and data security. The largest fine to date was NOK 65 million, imposed on Grindr for GDPR violations involving the disclosure of personal data to advertising partners, which has been contested in court. Datatilsynet operates under the Ministry of Local Government and Regional Development with an annual budget of NOK 82 million. Fine procedures involve formal notifications and opportunities for the company to respond before a final decision, which can be appealed. Fines are transferred to the state treasury. Datatilsynet uses EDPB guidelines for fine calculation but does not comprehensively publish all fines; however, significant decisions are made available upon request. In terms of legal consequences, Norway allows class actions, though these are rare due to stringent requirements and high litigation costs. Overall, fines remain more prevalent than private litigation in data protection matters.	its capacity for significant fines, as shown by the NOK 65 million sanction against Grindr. While class actions are permitted, they are infrequent due to high legal thresholds and costs, meaning administrative fines will remain the primary compliance mechanism. With an established focus on transparency, cybersecurity, and youth data, Norway's enforcement posture under the AI Act is likely to intensify, though within the bounds of its current regulatory and legal culture.
Poland	In 2024, the Polish Data Protection Authority (UODO) is focused on the processing of personal data in web applications, compliance with GDPR's information obligations, and ensuring adequate security measures to protect personal data. The new DPA, appointed in January 2024, is prioritizing citizens' rights and engaging with various sectors. UODO has increased fines for violations related to data security and breach notification, with notable cases including a PLN 1,440,000 fine for Santander Bank Polska for failing to notify a data breach. The most significant fine to date was PLN 4,911,732 against Fortum for inadequate security measures and poor oversight of a processor. UODO conducts inspections based on annual plans, focusing on businesses using mobile applications and ensuring GDPR-compliant Privacy Policies. While fines are often imposed, corrective measures like reprimands are more common. The UODO's budget was PLN 41.7 million in 2022, and fines are directed to the state treasury. Public authorities can also be fined, but the fines are capped for certain entities. UODO does not publish all fines but releases selected decisions, especially in high-profile cases. Class actions for data protection violations are not common in Poland, and fines are currently more impactful than private litigation, though this may change with increased enforcement of data subjects' rights.	Poland is likely to experience a medium-scale impact from EU AI Act enforcement fines, in line with its growing but cautious GDPR enforcement practices. The UODO has demonstrated its willingness to issue significant fines for security failures and breach mismanagement, while maintaining a balanced approach that often favors corrective measures like reprimands. With the appointment of a new DPA and increased focus on digital platforms and citizens' rights, enforcement under the AI Act is expected to intensify, especially in sectors involving high-risk AI. Although class actions are rare, enhanced enforcement tools may gradually elevate the role of administrative fines in ensuring compliance.
Spain	Fines cannot be imposed on public entities or authorities in Spain unless they are acting in a private capacity. The Spanish Data Protection Authority (AEPD) maintains high transparency in its fining decisions, anonymizing personal details while identifying the infringing companies. So far, fines imposed by the AEPD seem more impactful than damage claims, but the significance of damage claims, particularly in class actions, is expected to grow in the future. In 2023, the AEPD focused on personal data breaches, financial institutions, data protection rights, fraudulent contracting, telecommunications, and Internet services,	Spain is likely to see a medium to large-scale impact from EU AI Act enforcement fines, based on its assertive GDPR fining practices and strong regulatory transparency. The AEPD has issued substantial penalties, including multi-million euro fines against tech giants, and has prioritized issues highly relevant to AI, such as biometric data and data subject rights. Although fines cannot target public authorities unless acting privately, the AEPD's broad scope and independent operation position it to play a leading role in AI Act enforcement. With the pending introduction of collective redress,

	accounting for 89% of the total fines. The most significant fine to date was EUR 10,000,000 imposed on Google LLC in 2022 for violating Articles 6 and 17 of the GDPR, related to unlawful data transfers and hindering the right to erasure. The AEPD, which has a budget of almost EUR 19 million and 247 staff members, is independent from the government and operates with full autonomy. The fine procedure allows the authority to impose fines directly, with fines being allocated to the state treasury. While there is no official calculation methodology for fines, Organic Law 3/2018 provides factors that influence fine amounts, such as the impact on minors' rights. Public authorities cannot be financially fined unless acting in a private capacity. The AEPD publishes information about fines, particularly for significant cases, and provides aggregated data in its annual reports. Spain does not currently have class actions for data protection violations, but with the upcoming transposition of EU Directive 2020/1828, class actions could be possible. Currently, fines from the AEPD are more significant than court proceedings, but there is a trend toward more litigation, especially as consumer associations take legal action on behalf of consumers. The AEPD has also focused on the use of biometric data, issuing several sanctions and guidelines related to its processing.	litigation may grow, but administrative fines will remain the primary compliance driver.
Sweden	Sweden has two data protection authorities (DPAs): IMY, which oversees compliance with the GDPR, and PTS, which enforces cookie rules under the Swedish Act on Electronic Communications. IMY focuses on complaint-based supervision, especially in the private sector, and has stated that it will review its handling of complaints related to publication certificates under Swedish constitutional laws, particularly regarding companies that publish publicly available information on individuals. PTS, on the other hand, has been less active, initiating only a few cases related to cookies. IMY's significant fines include SEK 58 million for Spotify in 2023 for failing to properly inform users about how their data is used, and SEK 75 million for Google in 2020, later reduced to SEK 50 million, for mishandling data subject rights. Sweden's DPAs are structured under the Ministry of Justice (IMY) and the Ministry of Finance (PTS), with IMY having a 2024 budget of SEK 180 million and 140 employees, and PTS having a budget of SEK 153 million and 420 employees. Both authorities follow procedures that ensure targets have the opportunity to respond before fines are imposed, and fines are paid to Kammarkollegiet. There is no official fining model in Sweden, but the authorities likely follow EU guidelines on setting fines. Public authorities can be fined up to SEK 10 million for GDPR breaches. IMY and PTS both publish supervisory decisions, with IMY also providing aggregated statistics on fines in its annual reports. In 2023, IMY imposed fines totaling SEK 120.4 million. Sweden also has provisions for class actions and representative actions for collective legal claims under the Swedish Group Proceedings Act and the Swedish Act on Representatives' Actions for the Protection of The Collective Interests of Consumers. Fines are currently more significant than	Sweden is positioned for a moderate to significant impact from EU AI Act enforcement fines, given its structured dual-regulator system (IMY and PTS), established fining record, and procedural rigor. IMY has already issued large GDPR-related fines, notably against Spotify and Google, and shows capacity for high-value enforcement. The country's legal infrastructure supports administrative fines over litigation, though collective actions are available and may become more relevant over time. The evolving legal conflict between data protection and press freedom may shape the AI Act's interpretation in Sweden, especially for AI systems involving public data. Nonetheless, Sweden's regulatory maturity and transparency indicate readiness for active AI Act enforcement.

	court proceedings for damages or injunctions, although there is growing legal tension between data protection under the GDPR and Sweden's constitutional freedom of the press protections, with the Swedish Supreme Court reviewing a case on this conflict and a CJEU preliminary ruling pending.	
United Kingdom	The UK's Information Commissioner's Office (ICO) has focused its enforcement activities primarily on large-scale personal data breaches and non-compliant direct marketing practices, often triggered by just a few complaints. Significant fines have been imposed in sectors such as marketing, finance, insurance, credit, retail, and manufacturing. Notable fines include EUR 22 million for British Airways and EUR 20 million for Marriott due to inadequate security measures that led to personal data breaches; both fines were significantly reduced due to the financial impact of COVID-19 and the companies' mitigation efforts. These cases also spurred class actions, including a major settlement in the BA case involving 16,000 claimants. The ICO is also prioritizing areas like children's privacy and improper cookie use. Fines and enforcement actions are generally published on the ICO website with detailed information about the breaches and entities involved. The ICO, an independent public body sponsored by the Department for Science, Innovation and Technology, had a budgeted income of EUR 99 million for 2023/24 and employed 944 staff as of March 2022. Fine procedures begin with a notice of intent, followed by the opportunity to make representations before a final penalty is issued. Appeals can be made to the First Tier Tribunal and subsequently through higher courts. The ICO does not keep the fines; they are remitted to His Majesty's Treasury. Instead, the ICO is funded mainly through a data protection fee levied on controllers. A five-step fining methodology was introduced in 2024 to enhance transparency and proportionality. Public authorities can also be fined, such as the Ministry of Defence's EUR 466,440 penalty in 2023 for security failings. While fines remain impactful, the rise of class actions and court proceedings for damages—particularly in high-profile cases—signals a growing legal risk landscape for data controllers in the UK.	The United Kingdom is likely to experience a significant impact from AI Act-style enforcement, given the ICO's established fining capacity, transparent procedures, and growing experience with complex, high-profile cases. The ICO has already imposed large fines for data breaches and non-compliance, including against major players like British Airways and Marriott, and has introduced a structured five-step methodology for calculating fines, indicating a move toward greater consistency and proportionality. The UK's legal environment is also evolving, with an increase in class actions and group claims, which may reinforce or supplement regulatory enforcement. Although the ICO does not retain fine proceeds, its stable funding model and large staff enable sustained enforcement. Sectors such as marketing, finance, and defense—already targets for GDPR enforcement—may similarly face scrutiny under AI-related regulations. Overall, the UK is institutionally well-equipped for robust enforcement, suggesting a high level of preparedness and a strong likelihood of impactful penalties under future AI regimes.

Calls to action



Embed AI Governance into Core Business Strategy

Integrate AI risk management, accountability mechanisms, and ethical oversight into corporate governance frameworks. Treat AI compliance not as a technical afterthought but as a strategic imperative that aligns with long-term value creation and trust-building.

Operationalize Privacy-by-Design in AI Systems

Ensure all AI development follows privacy-by-design principles—minimizing data use, securing user consent, and enabling explainability. Implement continuous monitoring to identify and remediate risks across the AI lifecycle, especially in high-risk use cases.

Invest in Cross-Functional Compliance Capabilities

Establish interdisciplinary teams involving legal, data, IT, and operations to address evolving AI regulatory demands. Equip teams with training, clear responsibilities, and access to compliance tools that enable rapid response to audits or enforcement actions.

Leverage Regulatory Readiness as a Competitive Advantage

Turn compliance into differentiation. Use your AI governance maturity to build customer confidence, attract partners, and win public tenders. Early alignment with the EU AI Act can position your firm as a leader in responsible and trustworthy AI deployment.

Conclusion

The rise of AI regulation marks a pivotal shift in how data governance, privacy, and accountability are enforced in the digital age. As demonstrated by GDPR enforcement trends, regulators are prepared to act decisively when AI systems compromise individual rights or operate without sufficient oversight. The EU AI Act builds on this foundation, introducing stringent compliance requirements for high-risk AI and reinforcing the legal framework for trustworthy AI deployment. Together, these instruments are reshaping operational standards across sectors and elevating expectations around transparency, fairness, and risk management in automated systems.

However, regulatory impact will be shaped by organizational readiness. Many businesses still grapple with aligning AI technologies to legal standards, documenting AI logic, and applying robust safeguards for personal data. SMEs, in particular, may face disproportionate challenges due to resource limitations and limited in-house expertise. Without targeted support, these firms risk falling behind in compliance and innovation alike. Yet the cost of non-compliance—reflected in substantial GDPR fines and reputational harm—makes proactive adaptation essential.

Encouragingly, leading organizations across finance, healthcare, and tech are already embedding compliance by design. These early adopters illustrate that responsible AI governance is both achievable and beneficial. Through risk assessments, algorithmic audits, and ethical oversight, they're improving system integrity while maintaining regulatory alignment. Their example provides a roadmap for scalable, privacy-first AI implementation.

Ultimately, the EU AI Act is not just a compliance challenge—it's a strategic opportunity. Businesses that embrace these reforms will gain trust, differentiate ethically, and shape the emerging norms of AI accountability. By aligning AI strategies with regulatory demands, industry leaders can ensure their innovations are not only powerful but principled—laying the groundwork for globally trusted, rights-respecting AI ecosystems.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

CMS, (2024), ‘GDPR Enforcement Tracker Report 2024’, accessible at: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report (last accessed 2nd May March 2025)

European Parliament and The Council of the European Union, (2024), 2024/1689 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), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 29th March 2025)

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V