Institut européen
European Institute

Executive Master in EU Studies

The Interplay Between the GDPR and the AI Act: Legal Challenges and Regulatory Alignment

Supervised by Prof Mattias Wendel

Florence GRABER

2025

Table of contents

Abstract

With artificial intelligence (AI) technologies rapidly advancing, there have been critical discussions on their compatibility with fundamental rights especially those relating to privacy and data protection as enshrined in the EU Charter of Fundamental Rights. In the European Union (EU) this gets addressed through two major regulatory instruments: the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). This thesis explores how these two frameworks interrelate, complement or potentially conflict when applied to AI systems that process personal data. Analysing it from a legal perspective, it looks at the core provisions of the GDPR and the AI Act, explores their legislative intent and integrates relevant case law from the Court of Justice of the European Union (CJEU).

Particular attention is paid to the shared regulatory principles like transparency, accountability, risk-based governance and protections against automated decision-making. The research finds that even though both instruments share a common normative foundation and are designed to be complementary, they have differing regulatory logics being individual-rights-based versus system-level risk management which gives rise to structural overlaps and legal ambiguities. These include the challenge of establishing a clear legal basis for AI-driven data processing, managing overlapping oversight responsibilities and operationalizing rights like human oversight and algorithmic explainability.

The paper finally concludes that effective regulatory alignment between the GDPR and the AI Act is essential for the establishment of a trustworthy AI environment in the EU. It proposes ways for harmonization that would enhance legal certainty and uphold the EU's commitment to fundamental rights which then helps to ensure that innovation remains both responsible and human-centric.

1. Introduction

Artificial intelligence (AI) is one of the most transformative technologies of the 21st century. With it spreading across many sectors, from healthcare to law enforcement as well as finance, AI has the potential to significantly improve efficiency, accuracy and innovation. However, this technological advancement also comes with significant risks especially in terms of its impact on fundamental rights like privacy, data protection and non-discrimination. In the European Union (EU) two key legislative frameworks were put into force to address these concerns namely the General Data Protection Regulation (GDPR)[1] and the Artificial Intelligence Act (AI Act).[2]

This thesis explores the intersection of these two legal instruments with a focus on how the AI Act aligns with or diverges from the GDPR's principles and obligations. The central research question thereby is: *How does the AI Act align with or diverge from the legal principles enshrined in the GDPR especially concerning fundamental rights such as privacy and data protection?* This question is set within a broader debate on the ethical, legal and societal implications of AI in a data-driven society.

The main purpose is to evaluate the potential for harmonization between the two regulations and to assess whether the AI Act sufficiently addresses the unique challenges posed by AI technologies in relation to data protection. To achieve this, this thesis employs a doctrinal legal methodology by analysing statutory texts, regulatory guidance and including of key judgments of the Court of Justice of the European Union (CJEU) where relevant. Particular focus is put on high-risk AI systems which are subject to the most strict obligations under the AI Act and are most likely to intersect with GDPR-regulated data processing activities.

The existing literature on the subject includes analyses of the GDPR's robustness as a fundamental rights instrument as well as critiques of the AI Act's risk-based approach and potential regulatory gaps. Up until now not to many studies have provided a comprehensive comparison of the two frameworks through the lens of their practical implementation and

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

[2] 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) [2024] OJ L1689 (AI Act).

legal alignment. This thesis aims to fill that gap by systematically determining the points of convergence like impact assessments, risk-based regulation and accountability requirements. This shall also be achieved by highlighting areas of legal uncertainty or potential conflict particularly with respect to enforcement, legal bases for processing and automated decision-making.

The results are showing that even though the GDPR and the AI Act are intended to work in parallel and reinforce each other, they also make for a complexity of compliance demands for AI developers and deployers. This includes challenges in identifying consistent legal bases for data processing, managing overlapping supervisory authorities and ensuring adequate human oversight and transparency in AI-driven decisions.

This thesis is divided into six chapters. After this introduction, chapter two sets the foundation by examining the legal frameworks of the GDPR and the AI Act which includes their underlying principles, scopes and their objectives. The third chapter then explores the points of alignment between the two instruments, focusing on shared regulatory goals such as fundamental rights protection, transparency, accountability and risk-based governance. I chapter four the core legal challenges that arise at the intersection of these frameworks, supported by relevant case law and doctrinal analysis, are discussed. In the fifth chapter of the thesis there is an evaluation of the broader policy implications and reflection on the future trajectory of AI governance in the EU. In the end Chapter 6 offers concluding remarks and outlines key recommendations on how to achieve better regulatory coherence and safeguarding fundamental rights in an AI-driven environment.

2. The Legal Framework of the GDPR and AI Act

The 2016 GDPR provides for an extensive system for data protection and focuses on values like lawfulness, fairness, transparency, data minimization and accountability. Together with its restrictions against automated decision-making, the GDPR creates extensive individual rights like access, rectification and deletion of personal data.

First put forward by the European Commission in 2021, the AI Act was based on the ideas of a risk-based regulatory approach for artificial intelligence systems.[3] Particularly high-risk

[3] Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final.

applications involving biometric identity, law enforcement and employment, now come with strict rules including transparency, human oversight and risk management. The AI Act, however, is not focused on data protection itself.

A comparison of both concepts showcases potential limitations or tensions when it comes to their implementation. On one hand the GDPR highlights individual rights and data protection and on the other hand the AI Act takes a system-level risk route. Understanding these differences is critical for providing legal protection in the time of continuous technical development and especially with AI being on the rise.

2.1. The Charter of Fundamental Rights and the Key Principles of the GDPR

The General Data Protection Regulation is the main legal framework of the European Union for protection of personal data. Several fundamental ideas are defined explicitly in Article 5(1) GDPR which are derived from Article 5 of Council of Europe Convention No. 108 for the Protection of Individuals regarding Automatic Processing of Personal Data (1981).[4] These principles govern the interpretation and application of specific provisions und offer the basis for data protection laws within the EU.

The fundamental principles of personal data processing under the GDPR contain:

1) Lawfulness, fairness and transparency: Personal data must be processed legally, fairly and transparently and respect statutory laws as well as legitimate interests of data subjects.[5]
2) Purpose limitation: Data collection must have clear and specific purposes. Additional processing needs to be limited to activities related to the original purposes.[6]
3) Data minimization: Collection and processing of only necessary data to fulfill the stated purpose which limits both quantity and type.[7]
4) Accuracy: Personal data must be kept accurate, complete and needs to be regularly updated.[8]

[4] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS 108.
[5] GDPR, art 5(1)(a).
[6] GDPR, art 5(1)(b).
[7] GDPR, art 5(1)(c).
[8] GDPR, art 5(1)(d).

5) Storage limitation: No identifiable storage of data for longer than actually needed for the processing purposes.[9]
6) Integrity and confidentiality: Safekeeping of personal data by appropriate technical and organizational measures to avoid any unauthorized access or accidental loss.[10]

Additionally, according to the principle of accountability, as described in Article 5(2) GDPR, data controllers need to put measures in place to guarantee compliance with these core principles and to demonstrate proactively their compliance.[11]

It is also important to indicate that the GDPR operationalizes fundamental rights enshrined in the EU Charter of Fundamental Rights (CFR),[12] notably Article 8 which explicitly states the right to personal data protection. This right gives individuals the ability to control their personal information and requires data controllers and processors to handle personal data in a transparent and secure manner.

Nevertheless, the exact conceptual limits of the fundamental right to data protection[13] is not quite clear. The Court of Justice of the European Union emphasized a duality within Article 8 CFR which can be seen in the *Eifert*[14] and *Deutsche Telekom*[15] cases. The first paragraph of the Article lays out the general right to personal data protection which can be interpreted as a general ban against data processing unless specific requirements are satisfied as stipulated in Article 8(2) CFR. These conditions comprise of fairness, explicit purposes, consent or lawful justification. While attempting to balance data protection and permissible processing, this dual interpretation creates challenges when looking at Article 8(2) CFR's second sentence which establishes people's rights to access and correct their data and Article 8(3) CFR which requires independent oversight. Additionally, the Eifert judgment recognized that restrictions on these rights must comply with requirements under Article 8 of the European Convention on Human Rights (ECHR) and acknowledge the intersection

[9] GDPR, art 5(1)(e).
[10] GDPR, art 5(1)(f).
[11] Leonie Wittershagen, *'The Transfer of Personal Data from the European Union to the United Kingdom Post-Brexit'* (De Gruyter 2023) 32 – 37 <https://doi.org/10.1515/9783110988253> accessed 20 March 2025.
[12] Charter of the Fundamental Rights of the European Union [2012] OJ C 326/393.
[13] ibid, art 8.
[14] Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECR 2010 I-1106, paras 59 – 61.
[15] Case C-543/09 *Deutsche Telekom AG v Bundesrepublik Deutschland* [2011] ECR 2011 I-03441, para 66.

between the right to data protection (Article 8 CFR) and the right to private life (Article 7 CFR).[16]

A strongly debated principle under data protection law is the purpose limitation principle which has two components, one of which is the requirement that data controllers must clearly specify data processing purposes at the moment of data collection. The latter restricts subsequent data processing strictly to the initially stated purposes. The GDPR requires a compatibility assessment when data is being processed for any new purposes while the European Court of Human Rights has a "reasonable expectations" approach linked to the protection of private life under Article 8 ECHR.[17] Some national laws, like German law for example, have an even stricter interpretation requiring a particular aim.[18]

As society becomes increasingly digitally connected, the concept of "personal data" which covers any data related to an identified or identifiable individual, keeps broadening the scope of data protection. As a result, other fundamental rights that have historically been applied in similar contexts (e.g. freedom of business conduct, right to physical integrity, anti-discrimination rights) may become less relevant and be superseded by the fundamental right to data protection. This broadened interpretation risks making data protection into a "super-fundamental right" which could diminish the diversity, nuances and distinctiveness of other fundamental rights within digital environments.[19]

2.2. Objectives and Scope of the AI Act

Responding to growing concerns regarding the regulation and control of AI systems, various approaches to AI policy have emerged globally. A comprehensive and noteworthy legislative framework is the EU AI Act which intends to systematically address these specific challenges.

The EU has made one of its most ambitious legislative efforts with its AI Act to regulate AI technologies comprehensively. Its primary aim is to establish a unified regulatory environment that strikes a balance between innovation and competitiveness while reducing

[16] *Eifert* (n14) paras 51 – 59.
[17] Martin Westlund, 'The development of the right to privacy under the ECHR' (Master's Thesis in Public International Law, Uppsala Universitet 2018), 31 – 32 <http://www.diva-portal.org/smash/get/diva2:1257161/FULLTEXT01.pdf> accessed 20 March 2025.
[18] See for example *Kennzeichenerfassung* (2008) BVerfG 1 BvR 2074/05, 1 BvR 1254/07.
[19] Maximilian von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR' (2020) 6(4) EDPL 509, 509 – 510 <https://doi.org/10.21552/edpl/2020/4/7> accessed 22 March 2025.

potential risks and societal challenges brought by AI. The Act also aims to promote public trust in AI technologies and their development by setting clear rules and transparency standards and thereby promoting their widespread adoption across various sectors.

The focus of the EU AI Act lays on ensuring the ethical and safe use of AI systems within the EU all while protecting fundamental rights and European values.[20] This is to be achieved by using a risk-based approach which classifies AI systems into four different categories based on their potential harm and societal impact: [21]

- Unacceptable Risk: AI systems in this category are posing severe threats and are fully prohibited. These are applications which are likely to cause significant harm or disproportionately influence individual's behaviours and rights like government-operated social scoring systems or real-time biometric identification in public spaces.[22]
- High Risk: Considered as "high risk" are systems which post significant risks and require strict compliance before deployment. These systems need extensive prior testing, comprehensive documentation and adhere to high transparency standards. Such systems are normally used in sensitive areas such as critical infrastructure, healthcare, education, employment, financial services, migration, asylum as well as law enforcement. Keeping ethical standards, respecting fundamental rights and reliable and transparent operation must be ensured within these critical systems.[23]
- Limited Risk: AI systems classified under limited risk need to meet some specific transparency obligations. For instance, a user must be made aware that they are interacting with an AI system, especially if the interaction is not obvious. In this way the used can make informed decisions about if and to what extent they want to engage with AI-driven services and platforms.[24]
- Minimal Risk: For example, AI-enabled spam filters or gaming applications fall under the minimal risk category and generally face little to no regulatory oversight.

[20] AI Act, rec (7) and (8).
[21] AI Act, art 1.
[22] AI Act, art 5.
[23] AI Act, Art 6; AI Act, Annex III.
[24] 'AI Act' (*European Commission*, 18 February 2025) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 15 March 2025.

These applications usually do not have any direct impact on individual's rights or personal safety and as a concequence require limited regulatory scrutiny.[25]

The AI Act has numerous critical provisions to ensure that AI systems get used in responsible, transparent and accountable way:

- Conformity Assessments: High-risk AI systems need to be assessed for conformity to make sure they are compliant with regulatory requirements.[26] Depending on the system and risk level, these assessments can be carried out by the system providers themselves or any other independent third-party.[27]
- Post-Market Monitoring: In order to continuously assure compliance and assess the effectiveness and safety of their systems, providers of high-risk AI systems must establish and maintain post-market monitoring frameworks.[28] This shall ensure the systems compliance and evaluate ongoing performance as well as safety. The goal of this continuous oversight is to identify and mitigate emerging risks or unintended consequences as soon as possible.[29]
- Transparency and Information Obligations: Providers are responsible for clear communication to users about the functionalities, limitations and operational characteristics of high-risk AI systems to ensure informed and transparent interactions. This includes duties to offer clear documentation, user instructions and information about potential biases or limitations that exist within the AI models.[30]
- Governance and Enforcement: The European Artificial Intelligence Board (EAIB) was established to enable the effective implementation and supervision of the EU AI Act. It provides guidance, facilitates cooperation between member states and offers recommendations on the implementation and interpretation of the AI Act. Furthermore, national supervisory authorities are essential when it come to the enforcement of the regulations at the member state level to ensure adherence to EU standards and promoting consistent application across the EU.[31]

[25] ibid.
[26] AI Act, art 6(1)(b).
[27] AI Act, art 43.
[28] AI Act, art 17(1)(h).
[29] AI Act, art 72.
[30] AI Act, art 13.
[31] 'Governance and enforcement of the AI Act' (*European Commission*, 17 February 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement> accessed 15 March 2025 ; 'AI Board'

By creating an environment which prioritizes fundamental rights and ethical standards next to technological advancement, the EU AI Act can have a great effect on AI research, development and its use within the EU. It seeks to strengthen innovation and aims to position the EU as a global leader in responsible AI governance all while establishing robust safeguards to protect individuals and communities. Beyond that, the Act is expected to influence other global AI governance frameworks since other regions or organizations might harmonize their regulations with the European approach. This possible global impact emphasizes the significance of the EU AI Act not only as a regional policy instrument but also as a reference for international standards and best practices in AI regulation. [32]

2.2.1 Balancing Innovation and Risk Management

To realize its general objectives, the AI Act wants to balance innovation and the risks posed by AI technologies. As mentioned in the previous section, the EU AI Act seeks to balance two central objectives. First, the objective of fostering innovation in AI to drive economic growth and global competitiveness and second, the effective management of potential risks that come with AI technologies. The legislative framework should be designed to boost the societal benefits of AI all while safeguarding fundamental rights, security and safety across the EU.

The EU AI Act shows how important technological innovation and economic growth within the EU is to position Europe as a global leader in responsible AI development. Simultaneously it takes a proactive approach to risk management by making sure that AI systems do not compromise fundamental rights, democratic principles or overall well-being. The Act takes a straightforward and risk-based regulatory strategy to reach this dual objective. Its relationship to existing data protection frameworks especially the GDPR is clarified in itself. According to Article 2(7) of the AI Act, they work alongside each other rather than the AI Act trying to supersede existing data protection laws. This means that AI systems processing personal data have to simultaneously adhere to the specific regulatory requirement of the AI Act as well as the data protection provision established in the GDPR.

(*European Commission*, 24 March 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-board> accessed 24 March 2025.

[32] Manoj M, Remya M and Nitha T M, *The New Intelligence: Exploring the AI Revolution* (Xoffencer international book publication house 2025), 129 – 131.

If both regulations overlap, the GDPR has primacy when it comes to personal data processing. The AI Act afterwards specifically addresses AI-related issues. [33]

Taking a constitutional approach the EU AI Act shows its potential for future evolution, especially in the case of automated decision making. Historical and national contexts can provide essential lessons and possibilities for reform. At national and EU levels, ongoing legislative changes can be analysed in light of broader constitutional principles by using the concept of the rule of law as a foundational framework. This viewpoint allows for a comprehensive understanding of the EU AI Act's ability to change regulatory landscapes, impact constitutional arrangements and direct future policy developments. [34]

2.2.2 High-risk AI systems and their regulation

A significant part of the AI Act's regulatory strategy is its detailed treatment of high-risk AI systems which demand special attention due to their potential impact on fundamental rights. Over the past decade, AI has remarkably grown and diversified, thereby also had an impact an almost every economic sector. AI provides great opportunities for growth, innovation and addressing societal challenges due to the ongoing digital transformation. This is especially remarkable in areas like environmental management, energy efficiency, agriculture optimization and healthcare. AI has grown to get a central position in policy frameworks within the EU, which were supported by extensive legislative initiatives and dedicated funding, all of this to tackle data driven innovation. The EU's approach shows a more human-centered view of AI and recognizes the need to align technological innovation with fundamental rights, safety and human health. By recognizing the challenges that the regulation of AI poses, the EU AI act shows a structured, risk-based approach where AI systems are classified on their potential risk to fundamental rights and societal well-being which enables precise and targeted governance. Systems involving invasive real-time biometric surveillance or social scoring systems, for example, pose unacceptable risks and are specifically prohibited as they conflict with EU core values and fundamental rights. [35]

---

[33] AI Act, recs (9) and (10); Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework of 16 July 2024 [2024], 2 <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> accessed 3 April 2025.
[34] Manon Punie, 'The GDPR and the AI Act: A Harmonized Yet Complex Regulatory Landscape' (*datenschutznotizen*, 22 January 2025) <https://www.datenschutz-notizen.de/the-gdpr-and-the-ai-act-a-harmonized-yet-complex-regulatory-landscape-1151788/> accessed 24 March 2025.
[35] Isabelle Hupont, Marina Micheli, Blagoj Delipetrev, Emilia Gómez and Josep Soler Garrido, 'Documenting High-Risk AI: A European Regulatory Perspective' (2023) 56(5) Computer 18, 18 – 19 <https://dx.doi.org/10.1109/MC.2023.3235712> accessed 25 March 2025.

As described in the foregoing part, the main focus of regulatory efforts are high-risk AI systems due to their potential significant impact on individuals and their fundamental rights. They are only allowed within strict regulatory compliance frameworks which are built of strict conformity assessments, transparency standards and monitoring requirements. In the AI Act such systems are explicitly defined based on their intended purposes and deployment contexts. Details regarding the classification and corresponding examples of high-risk AI systems can be found in Annex III which offers in which areas AI systems were identified as posing immediate or likely imminent risks to fundamental rights. High-risk AI systems need to follow the comprehensive regulatory requirements defined under Chapter III of the Act which state that providers are obliged to conduct mandatory conformity assessments to ensure adherence to established safety, accuracy and transparency standards before deploying these systems. Also, there are some transparency and explainability obligations which require providers to clearly communicate the capabilities, limitations and operational characteristics of AI systems to regulatory authorities and users. High-risk AI systems also need to be continuously surveyed to make sure the emerging risks, performance issues or any other unforeseen consequences get addressed in real-time operations effectively.[36]

The EU AI Act is strongly emphasizing the safeguarding of fundamental rights to prevent biases or unclear decision-making from affecting these rights. Strong data governance techniques such as safeguards against bias and discrimination in AI systems, have to be put in place by providers in order to ensure compliance. This means upholding equality and fairness across datasets and operational parameters in accordance with the fundamental rights and values of the EU. To foster innovation and widespread acceptance of AI technologies, the EU aims to establish broad public trust and encourage the ethical application of AI through high transparency, clear communication and strict governance measures.

With its risk-based approach, classifying AI systems based on the degree of risk they pose to fundamental rights and other protected interests, the EU recognizes the particular difficulties in regulating AI. Different regulatory requirements apply depending on the level of risk which can range from minimal to high or even unacceptable. For instance, Title III of the European Commission's Proposal laid out specific regulations pertaining to high-risk AI.[37] High-risk AI systems are classified based on their intended purpose with detailed

[36] AI Act, art 8ff.
[37] n 3.

typologies as described in Annex II and a list of particularly sensitive applications included in Annex III. AI systems need to be unbiased in their decision-making and data evaluation procedures to prevent discriminatory results and fundamental rights to be protected sufficiently. Strict governance and oversight are necessary as such protection becomes especially difficult in situations where there is little transparency or a lack of knowledge about the internal mechanisms of an AI application.[38]

2.3 Conclusion

Although protecting fundamental rights in the digital age is the goal of both the GDPR and the AI Act, their opposing regulatory logics reveal underlying tensions that complicate their coexistence. The GDPR places a strong emphasis on consent, individual autonomy and strict purpose limitation which are principles which compete with the data-driven, adaptive nature of many AI systems. On the other hand, the AI Act places more emphasis on enabling innovation and systemic risk management, often without providing any specific safeguards for the granular rights outlined in the GDPR. Particularly in high-risk AI applications where personal data is central but individual rights may be difficult to enforce in practice, this asymmetry runs the risk of generating regulatory blind spots. Furthermore, questions concerning accountability, transparency and the adequate level of oversight are raised by the AI Act's reliance on technical assessments and provider self-regulation. Ultimately, ensuring effective regulatory alignment while preserving fundamental rights requires ongoing interchange between legal norms, technical innovation and democratic values.

3. Regulatory Synergies Between the GDPR and the AI Act

Though they have their differences in regulation and scope, the GDPR and the AI Act share several core objectives as both want to make sure that technological advances especially those involving personal data, are carried out safely, transparently and respectfully regarding fundamental rights. Therefore, the two systems support one another by reinforcing common regulatory principles and help to provide more legal certainty for AI users and developers.

The present regulatory framework around the AI Act reflects the atmosphere that came before the GDPR was implemented in many ways. Just as companies once needed to race to align their operations with the requirements of the GDPR, a similar shift is now going on as

[38] Jon Truby, Rafael Dean Brown, Imad Antoine Ibrahim and Oriol Caudevilla Parellada, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications' (2021) 13 European Journal of Risk Regulation 270, 274 <https://ssrn.com/abstract=4373418> accessed 23 March 2025.

businesses prepare to comply with the AI Act. Especially in the way of how they control the intersection of data, technology and fundamental rights. Both instruments present significant developments in EU law. The GDPR and the AI Act also reflect similarities in regulation by both taking a risk-based, principle-driven approach that balances the protection of individual rights and the encouragement of innovation. They set strict enforcement policies and require thorough compliance including huge fines for non-compliance. Though the GDPR is specifically concerned with the protection of personal data, the AI Act addresses concerns outside of only data protection by extending its reach to the ethical and safe use of artificial intelligence systems as a whole.[39]

3.1. Common Ground: Fundamental Rights Protection

The main objectives of the GDPR and the AI Act are fundamental rights. As mentioned before, the GDPR explicitly recognises data protection as a fundamental right under Article 8 of the EU Charter of Fundamental Rights, the AI Act then emphasises adherence to fundamental rights as a fundamental requirement for AI systems, especially high-risk systems.

The AI Act enhances GDPR protections by making AI systems handling personal data to adhere to existing EU data protection laws.[40] This guarantees that AI models which are being used in sensitive industries like healthcare, law enforcement and finance do not violate people's privacy or discriminate against them in any way. Additionally, the AI Act operationalises the protection of fundamental rights as a core part of AI deployment by incorporating a specific requirement under Article 27 which is the Fundamental Rights Impact Assessments (FRIAs) for high-risk AI systems. FRIAS are looking at the possibility and seriousness of possible harm to people's rights and determining the appropriate mitigating actions and thereby concentrate on managing the risks instead of entirely eliminating it. By addressing more general, AI-specific risks like opacity, bias and autonomy, this extends the current risk assessment culture which is based on the GDPR's Data Protection Impact Assessment (DPIA), into the AI domain.[41]

---

[39] Tijana Žunić Marić, Jelena Đukanović and Danilo Spasojević, 'Comparing the obligations under the GDPR and AI Act - where is the overlap?' (*lexology*, 22 October 2024) <https://www.lexology.com/library/detail.aspx?g=5487aa15-1408-4564-bcfe-7138a3869268#> accessed 23 March 2025.

[40] AI Act, art 2(7).

[41] Thomas Ajoodha and Jared Browne, 'Fundamental Rights Impact Assessments: What are they? How do they work?' (2025) CEDPO AI and Data Working Group Micro-Insights Series January 2025, 4 <https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf> accessed 28 March 2025.

This shared foundation contributes to a coherent legal framework that balances AI innovation with the protection of human rights and underlines the EU's constitutional commitment to privacy, dignity and equality.

3.1.1. Data Protection Impact Assessments

A DPIA is a key compliance and risk-management tool under the GDPR. Introduced formally in 2018, the DPIA is a process designed to identify, analyse and mitigate the risks that personal data processing activities might pose to the rights and freedoms of individuals. The primary purpose of a DPIA is to ensure that data protection risks are thoroughly assessed and appropriately addressed before high-risk processing operations begin. This includes considering the necessity and proportionality of data processing in relation to its purposes as well as evaluating the potential adverse effects on data subjects.[42]

Most importantly a DPIA goes beyond legal compliance as it also serves as a tool for responsible decision-making, transparency and public trust. DPIAs are mandatory when a project is likely to present a high risk to individuals' rights and freedoms. High-risk scenarios can for example include large-scale processing of special categories of data such as health or biometric data or systematic monitoring or profiling. Even when not legally required, conducting a DPIA is often encouraged as best practice to demonstrate accountability and to improve the overall quality and sustainability of a project. The process of conducting a DPIA typically follows a structured methodology and results in a comprehensive report. According to the GDPR, a DPIA must include a systematic description of the foreseen processing operations and their purposes, an assessment of the necessity and proportionality of the processing, an evaluation of the risks to data subjects and the measures predicted to address those risks and ensure compliance with the GDPR.[43] These elements help ensure that organisations approach personal data processing in a thorough, transparent and rights-respecting manner. Importantly, the DPIA must be conducted before processing begins, to ensure its findings can still meaningfully influence the project design. Failure to conduct a DPIA where needed can result in significant regulatory consequences which can be

[42] 'What is a DPIA?' (*ico. Information Commissioner's Office*) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/> accessed 31 March 2025.
[43] GDPR, art 35.

administrative fines of up to €10 million or 2% of the global annual turnover.[44] Also, inadequate or incorrect DPIAs have already led to penalties by data protection authorities.[45] Overall, the DPIA is not only a compliance requirement under the GDPR but also as a strategic instrument to enhance legal certainty, foster ethical processing practices and support the alignment between innovation and fundamental rights in data-driven projects.

3.1.2. AI and the Fundamental Rights Impact Assessment

As mentioned in the introduction of this chapter, the GDPR and the AI Act are both aiming to safeguard individuals' fundamental rights in a data-driven society. The GDPR recognizes data protection as a fundamental right with "the protection of natural persons in relation to the processing of personal data is a fundamental right"[46] identifying data protection not just as a matter of compliance but as an expression of human dignity and autonomy as guaranteed by the EU Charter.[47] The AI Act is similarly rooted in European value with its very purpose being human-centric and trustworthy AI that upholds "a high level of protection of […] fundamental rights as enshrined in the Charter of Fundamental Rights".[48]

From the outset, the AI Act underlines that it does not override or affect the application of existing data protection law. [49] Instead, by addressing the kinds of risks and rights impacts that are unique to AI technologies, it is designed to complement and expand the GDPR. The requirement that deployers of high-risk AI systems, especially public sector organisations and private actors providing public services, conduct a Fundamental Rights Impact Assessment before implementing such systems is important to reach this goal. While developers of AI systems will have already conducted preliminary risk analyses, it is ensured through the FRIA that any risks materializing at the level of concrete deployment are also identified and mitigated. This is based on knowledge that some harms only manifest themselves in particular operational contexts and a number of crucial factors need to be taken into consideration by the FRIA. This includes the system's intended use and the processes it will support, the frequency and duration of its use and the groups and individuals that are most likely to be impacted. Potential harms must also be identified and consequently methods for monitoring, supervising and reducing these risks be suggested. To guarantee

[44] GDPR, art 83(4).
[45] Thibaut D'hulst and Dariusz Kloza,'Data protection impact assessment: More than just a compliance tool' (*Van Bael & Bellis,* 25 November 2022), 3 and 4 <https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf> accessed 28 March 2025.
[46] GDPR, rec (1).
[47] GDPR, rec (2).
[48] AI Act, rec (1).
[49] AI Act, rec (10).

that violations of fundamental rights can be promptly addressed, measures like internal governance structures and complaint mechanisms need to be implemented. These responsibilities show a growing understanding that algorithmic systems, especially those that make or support life-altering decisions, need to be governed with a strong focus on human rights, accountability and transparency. [50]

Crucially, the FRIA requirement in the AI Act is not a stand-alone requirement. It is intended to work in tandem with and enhance other regulatory tools, particularly the GDPR's Article 35 Data Protection Impact Assessment. While the FRIA covers a wide range of fundamental rights such as equality, freedom of expression, access to justice and protection from discrimination, the DPIA focusses exclusively on risks related to the processing of personal data. Article 27(4) of the AI Act adds complementarily to the Digital Services Act, stating that if certain obligations under the FRIA are already fulfilled through a DPIA, the FRIA will build upon and extend that assessment to ensure comprehensive rights protection. This goes along with a broader trend in EU digital regulation which aims to integrate multiple layers of impact assessment for holistic and proactive governance of emerging technologies. The aim is not only to prevent violations but to instill a culture of anticipatory and responsible innovation.[51]

Overall, the AI Act and the GDPR both uphold the idea that human rights must be respected and protected in the process of technological development. A strong framework for legal data processing based on privacy and equity is provided by the GDPR and the AI Act expands that protection to include algorithmic system design, development and deployment. Both together provide a strong legal foundation that guarantees the EU's core principles of freedom, equality and dignity will still be focused on in the era of artificial intelligence. While DPIAs and FRIAs reflect the operationalization of fundamental rights protections, they also reveal a deeper alignment between the two frameworks' conceptualizations of regulatory duty. This shared foundation prompts a closer look at their risk-based approaches.

[50] Thomas Ajoodha and Jared Browne, 'Fundamental Rights Impact Assessments:
What are they? How do they work?' (2025) CEDPO AI and Data Working Group Micro-Insights Series January 2025, 7 and 8 <https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf> accessed 28 March 2025.
[51] ibid.

3.2. Risk-Based Regulatory Approaches

Despite the differences in the GDPR and AI Act's mechanics and scope, their regulatory approaches are complementary and remain risk-based in a similar way. The GDPR is a horizontal regulation that applies to the processing of personal data in all sectors and is technology-neutral. It lays out the ground rules and ex-post enforcement. Organizations are required to create compliance programs (designate DPOs, carry out Data Protection Impact Assessments, etc.) and may face penalties for noncompliance. In contrast, the AI Act is a vertical tech-focused law that is modelled on product safety regulations. Based on risk areas, it establishes an ex ante compliance regime for AI systems: low-risk AI may be subject to transparency requirements, high-risk AI systems must meet stringent requirements prior to deployment and unacceptable-risk AI practices are prohibited. The two laws were "designed to work hand-in-glove" despite these differences.[52] While the GDPR is a fundamental rights law that gives individuals several rights in relation to the processing of their data the AI Act primarily ensures the technical robustness and safety of AI only directed to individual rights in a limited way. Thus, the AI Act relies on the GDPR to fill any gaps in individual rights protection when AI systems use personal data. The AI Act's categorization of AI by fundamental rights risk echoes the GDPR's requirement to match data protection measures to the risk to individuals. Together, they create a unified risk-based approach that bridges general data governance and AI-specific risks.[53]

Their alignment is further shown through how the roles and responsibilities interplay under each framework. While organizations that create or implement AI may be providers (creators/suppliers of AI systems) or deployers (operators using AI) under the AI Act, they may be considered controllers or processors of personal data under the GDPR. A deployer who uses an AI system on personal data will also be a GDPR controller which shows the analogy between these role concepts. Importantly, an organization is not exempt from the other law just because it complies with one of them. The AI Act makes it clear that any processing of personal data by AI providers and deployers is still subject to data protection laws. [54] This means, that even though the AI Act imposes additional requirements on the AI

[52] James Clark, Muhammed Demircan and Kalyna Kettas, 'Europe: The EU AI Act's relationship with data protection law: key takeaways' (*DLA PIPER*, 25 April 2024) <https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/> accessed 31 March 2025.

[53] Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024) 54 Computer Law & Security Review 106020, 2 – 4 <https://doi.org/10.1016/j.clsr.2024.106020> accessed 24 March 2025.

[54] AI Act, art 2(7) and rec (69).

system itself, all requirements associated with being controller or processor under the GDPR remain applicable.

Conversely, if a high-risk AI system processes personal data, one precondition for its lawful deployment is that GDPR requirements are met. The European Data Protection Board (EDPB) stressed in its opinion of the AI proposal that adherence to GDPR "should be a precondition to being allowed to enter the European market" as an AI system.[55] This ensures a coordinated approach as for example a business may be required to complete a conformity assessment under the AI Act and prove GDPR compliance (e.g. completing a DPIA and implementing privacy safeguards) prior to deploying a high-risk AI tool. Many mechanisms overlap in practice as for example both laws require impact assessments: the AI Act (Article 27) requires a Fundamental Rights Impact Assessment for many high-risk AI systems and GDPR (Article 35) requires a Data Protection Impact Assessment for high-risk personal data processing. Although they cover different areas, these evaluations are complementary to one another: the AI Act's FRIA covers broader effects on the rights and freedoms of individuals while the DPIA focusses on personal data and privacy risks. Together they force businesses to carefully assess AI systems for potential issues prior to implementation.[56]

Enforcement and governance structures under the two regimes are also being aligned to reinforce one another. The GDPR established independent Data Protection Authorities (DPAs) in each state and the EDPB to ensure consistent interpretation. The AI Act likewise envisages national supervisory authorities for AI and a new European AI Board to coordinate them, paralleling the one-stop-shop cooperation model of the GDPR. Notably, the EU's data watchdogs have argued for strong cooperation between these bodies – even suggesting that DPAs be designated as AI regulators – to leverage their expertise in fundamental rights oversight. While the AI Act enforcement will incorporate product safety regulators and market surveillance authorities, data protection regulators will continue to play a critical role

[55] Joint Opinion 5/2021 of 18 June 2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2021], 10 <https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 31 March 2025.

[56] Thomas Ajoodha and Jared Browne, 'Fundamental Rights Impact Assessments: What are they? How do they work?' (2025) CEDPO AI and Data Working Group Micro-Insights Series January 2025, 4 – 8 <https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf> accessed 28 March 2025.

whenever AI systems process personal data.[57] Indeed, DPAs have already been at the forefront of policing AI under the GDPR even before the AI Act comes into force, targeting issues like unlawful data collection, lack of transparency or bias in algorithms. For example, GDPR enforcement actions have tackled an AI-based facial recognition database built on web-scraped images which also raise concerns addressed by the AI Act's high-risk categories (biometric AI).[58] Going forward, an AI system that violates the AI Act's requirements, e.g. by lacking transparency or sufficient risk controls, may simultaneously be violating GDPR principles like fairness or purpose limitation if personal data is involved. Non-compliance risks are correspondingly significant: the AI Act introduces fines that can reach €35 million or 7% of global turnover[59] for the most serious breaches, exceeding the GDPR's maximum 4%.[60] This dual accountability creates a powerful incentive for organizations to adopt an integrated compliance approach.

In conclusion, even though the GDPR and AI Act have different regulatory approaches with one being an omnibus data protection law while the other one is a lex specialis for AI, they are designed to complement each other. The GDPR's established enforcement framework supports the adoption of the AI Act which builds upon its foundation by integrating data protection principles into AI governance in its own way. Their combined regulatory approach is layered but harmonious with the AI Act adding traffic signals unique to AI technology to prevent new forms of harm while the GDPR gives general guidelines for personal data and individual rights.

3.3. Joint Transparency and Accountability Mechanisms

Transparency and accountability are core obligations under both the GDPR and the AI Act, and there is considerable overlap in what they require of organizations. The GDPR mandates transparency in all personal data processing: personal data must be processed "fairly and in a transparent manner".[61] In practice this means data controllers must provide clear notices

[57] Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework of 16 July 2024 [2024], 2 and 3 <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> accessed 3 April 2025.
[58] 'Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition' (*Autoriteit Persoonsgegevens*, 3 September 2024) <https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition> accessed 12 April 2025.
[59] AI Act, art 99.
[60] GDPR, art 83.
[61] GDPR, art 5(1)(a).

to individuals about how their data is used, ensure data subjects can access and receive information on their data[62] and generally make processing understandable.[63]

The AI Act echoes and broadens this principle. The AI Act ensure that people are being made aware of how AI is affecting or interacting with them by introducing transparency requirements specific to AI systems. The Act for example mandates that users have to be informed when interacting with AI systems. If someone is interacting with an AI chatbot or viewing content created by AI, they must be informed that the respective content is machine-generated. Similarly, AI that creates deepfakes or synthetic media, needs to make its nature very clear.[64]

By focusing on the nature of the technology, these provisions complement the transparency of the GDPR. They protect the right of individuals to know that AI is being used which is closely related to the GDPR's right to know how their personal data is used. Both regimes are applicable in situations where an AI system handles personal data and the data subject would be given a GDPR privacy notice that details the data, recipients and purposes of the data as well as any disclosures specific to AI such as a notification that an algorithm and not a human is making certain assessments. When combined, these make sure that people are being informed about data-driven decisions which affect them. In addition to providing information to individuals, both laws require organisations to be accountable which includes proactive compliance measures and internal transparency in the form of documentation. The GDPR's accountability principle[65] makes controllers responsible for compliance with all data protection rules and they are obliged demonstrate it.[66] The implementation of "data protection by design and by default" impact assessments which entail the appointment of Data Protection Officers and the maintenance of processing records, are some measures that operationalize this.[67] A thorough accountability framework for high-risk AI systems is provided for by the AI Act. Providers of such AI are required to maintain thorough technical documentation, log the AI system's operations for traceability and put in place strict risk and quality management systems.[68]

---

[62] GDPR, arts 12 – 15.
[63] Ljubiša Metikoš and Jef Ausloos, 'The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act' (2025) 17(1) Law, Innovation and Technology, 8 <https://doi.org/10.1080/17579961.2025.2469349> accessed 11 April 2025.
[64] n 24.
[65] GDPR, art 5(2).
[66] 'Accountability' (*European Data Protection Supervisor*) <https://www.edps.europa.eu/data-protection/our-work/subjects/accountability_en> accessed 1 April 2025.
[67] GDPR, art 25.
[68] AI Act, art 9ff.

These regulations closely resemble GDPR mechanisms. For example, the AI Act's requirement to keep logs and documentation is similar to the GDPR's record-keeping obligations and the requirement that organizations provide evidence of compliance. In fact, the AI Act specifies that by establishing particular guidelines for "transparency, technical documentation and record-keeping of AI systems" which enhances the effectiveness of already-existing rights and remedies.[69] This is similar to how the GDPR requires controllers to be prepared to prove compliance to supervisory authorities, regulators or auditors which may then look at this thorough documentation.

Another area of convergence is transparency with regulators. As mentioned in Chapter 4.1.1., organizations are obligated to work with DPAs and may be asked to disclose their processing activities and DPIA reports under the GDPR.[70] Similar to this, the AI Act mandates that critical information about high-risk AI systems be entered into a publicly accessible EU database. This could be the main details of the system's deployment, goal and compliance protocols.[71] A summary of the data protection impact assessment conducted under the GDPR is even to be included in this database entry, where applicable, highlighting the practical interdependencies between the two regimes.[72] Notably, both frameworks are talking about the issue of human accountability. The GDPR explicitly notes the principle of human oversight through governance roles like the DPO mentioned in Article 37 GDPR and implicitly through the right to human intervention in automated decisions in Article 22 GDPR.[73] According to the AI Act, high-risk AI systems must be designed and monitored in a way that allows humans to meaningfully oversee the AI's operation and intervene or disable it if it wrongfully threatens rights or safety.[74] This requirement aligns with the GDPR's safeguards for data subjects against unchecked automation. Both laws essentially state that organizations cannot transfer accountability to algorithms. The message is the same whether viewed through the lens of the GDPR, which treats AI outputs as decisions for which a controller is responsible or the AI Act, which expressly calls for human control and oversight mechanisms. It can be said that those who use AI must maintain accountability for its impacts.

---

[69] AI Act, rec (9).
[70] GDPR, art 35.
[71] AI Act, art 49; AI Act, Annex VIII.
[72] AI Act, Annex VIII s C.
[73] Anna Levitina, 'Humans in automated decision-making under the GDPR and AI Act' in Carme Colomina Saló, Daniel Innerarity and Marta Cantero Gamito (eds.), *Algorithmic inequality: governance, representation and rights in AI* (CIDOB 2024), 126 <https://www.cidob.org/sites/default/files/2025-02/121-143_ANNA%20LEVITINA_ANG.pdf> accessed 19 April 2025.
[74] AI Act, art 14; ibid 132.

Ultimately, the two instruments reinforce the transparency of each other's enforcement. The GDPR requires data controllers to notify authorities and even impacted individuals of certain data breaches which may include instances in which an AI system misuses personal information.[75] The AI Act also mandates that significant incidents or malfunctions of high-risk AI systems have to be recorded and reported to authorities.[76] Additionally, the AI Act complements the investigative authority granted to DPAs under the GDPR by enabling authorities to request access to training data or source code for investigation which is subject to safeguards.[77] Under either regime, noncompliance may lead to decisions about public sanctions which encourages transparency about the standards that are expected.

In conclusion, the GDPR and AI Act interact to promote a culture of transparency and accountability in the use of AI through a variety of overlapping obligations ranging from giving notices and explanations to maintaining thorough records and enabling oversight. An organization following GDPR's accountability principle like documenting decisions or managing data responsibly, will find that those efforts directly support AI Act compliance and vice versa. Through common processes this collaboration not only reduces the burden of compliance but more significantly ensures that data processing and AI system operation continue to be transparent, auditable and subject to legal and ethical standards. Whilst transparency and accountability obligations are the backbone of both frameworks, this is even more important when decisions are made without direct human involvement. The next section therefore turns to the legal and ethical safeguards in place to protect individuals automated decision-making and profiling practices that could potentially be harmful.

3.4. Protection Against Automated Decision-Making and Profiling

The GDPR and AI Act are sharing the common goal to protect individuals from the risks of automated decision-making and profiling, thereby ensuring that such processes do not undermine human autonomy or equality. People have the right under the GDPR not to be subject to a decision that has legal effects or similarly significant effects and is based only on automated processing, including profiling.[78] This right embodies a fundamental safeguard as there is, unless an exception applies, a general prohibition to decisions that are

[75] GDPR, arts 33 – 34.
[76] AI Act, art 73.
[77] AI Act, art 74(12).
[78] GDPR, art 22(1).

solely algorithmic and have the potential to seriously impact an individual which could be for example an automated credit denial or e-recruitment filtering without any human oversight.[79] Even when there are exceptions regarding automated decisions such as explicit consent, contract necessity or law authorization, the GDPR mandates the implementation of protective measures. These include information about the automated process, allowing the individual to "obtain human intervention, to express [their] point of view, to obtain an explanation of the decision reached […] and to challenge the decision".[80] It is also mandated that controllers who use profiling or AI for important decisions need to undertake measures to ensure fairness. This can be for instance, by using "appropriate mathematical or statistical procedures" correcting inaccuracies in data and preventing discriminatory effects on protected groups.[81] In short, the GDPR sets a baseline that individuals must not be victims of unchecked, opaque algorithms and they retain a right to be involved or have another human involved and to expect non-discrimination in algorithmic decisions.[82]

These safeguards are extended upon and applied to particular AI contexts by the AI Act. It tackles automated decision-making by enforcing controls on high-risk applications and outlawing the most harmful types. Notably, unacceptable AI practices such as certain forms of automated decision-making that are thought to be essentially contradictory to EU values, are as previously mentioned, prohibited by the AI Act. It also, for instance, prohibits AI systems that use subliminal techniques to manipulate people or that assess or rate someone's credibility through so-called social scoring systems. The AI Act's prohibition of social scoring which is essentially extreme profiling by governments, supports the GDPR's objectives to stop arbitrary or unfair profiling of people. The use of AI for law enforcement's real-time remote biometric identification of individuals in public is another practice that is only allowed with very limited exceptions.[83] This is in line with concerns about automated surveillance and profiling of people in public areas, where data protection authorities have also warned that indiscriminate facial recognition would violate the GDPR and Charter's principles of necessity and proportionality. The AI Act effectively hard codes into law the

[79] GDPR, rec (71).
[80] ibid.
[81] ibid.
[82] 'Artificial Intelligence and automated individual decision making, including profiling, under Art. 22 GDPR' (*fieldfisher*, 30 June 2023) <https://www.fieldfisher.com/en/insights/artificial-intelligence-and-automated-individual-decision-making> accessed 10 April 2025.
[83] AI Act, rec (32) and (33); Tambiama Madiega, 'Artificial intelligence act' [2024] European Parliamentary Research Service, 3 <https://www.dirittobancario.it/wp-content/uploads/2024/09/Documento-riassuntivo-dellAI-Act-Parlamento-europeo-settembre-2024.pdf> accessed 10 April 2025.

kind of outcome that the GDPR's fairness and rights provisions would also achieve by prohibiting or severely restricting these uses, ensuring that certain automated processing which affects individuals is not allowed. For automated AI decisions that are allowed, which means they are high-risk and not completely banned, the AI Act imposes a number of safeguards which closely aligns with GDPR's protections.[84] All high-risk AI systems that make decisions about individuals, like AI used in creditworthiness assessment, hiring or educational evaluations, must be designed in a way that ensures the capability of human oversight.[85] This means that the respective AI should not operate as an unchallengeable "black box"[86] and human operators must be able to understand its outputs to a reasonable degree and intervene if necessary. This requirement interlinks with the GDPR's mandate for human intervention upon an individual's request creating a double layer of oversight as the system is built to make human controls possible and the individual can demand a human review. Moreover, the AI Act mandates providers to ensure such systems are accurate, explainable and unbiased.[87] For example, high-quality training data needs to be used to minimize errors and discriminatory impacts.[88] This echoes the aforementioned instruction in the GDPR Recital 71 that profiling should avoid errors and "prevent […] discriminatory effects" on protected classes.

Through these requirements, the AI Act tackles the algorithmic conditions that could lead to unfair automated decisions as it aims to pre-emptively reduce the risk of biased or erroneous outputs while the GDPR gives individuals post-hoc rights to contest and inquire into those decisions. The instruments thus work together in the way that the AI Act pushes developers and deployers to prevent harmful automated decisions by building AI systems to certain standards and the GDPR empowers individuals to remedy or resist harmful decisions if they happen.

---

[84] AI Act, art 8ff.
[85] AI Act, art 14; AI Act, rec 73.
[86] "…, these black box models are created directly from data by an algorithm, meaning that humans, even those who design them, cannot understand how variables are being combined to make predictions. Even if one has a list of the input variables, black box predictive models can be such complicated functions of the variables that no human can understand how the variables are jointly related to each other to reach a final prediction." in Cynthia Rudin and Joanna Radin, 'Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition' (2019) 1(2) Harvard Data Science Review, 3 <https://doi.org/10.1162/99608f92.5a8a3a3d> accessed 10 April 2025.
[87] Cecilia Panigutti, Ronan Hamon, Isabelle Hupont and others, 'The role of explainable AI in the context of the AI Act' (Conference: FAccT '23: the 2023 ACM Conference on Fairness, Accountability, and Transparency, June 2023), 1142 <https://dl.acm.org/doi/pdf/10.1145/3593013.3594069> accessed 10 April 2025.
[88] n 24.

3.4.1. Right to explanation

Their complementarity is clearly shown by the new "right to an explanation" introduced in the AI Act. The AI Act grants anyone affected by a significant decision based on a high-risk AI system the right to get a "clear and meaningful explanation of the role of the AI system in the decision-making procedure and the main elements of the decision taken".[89] This is a significant provision that essentially guarantees that people can understand how the AI influenced a decision that has a significant impact on their safety, health or fundamental rights. Notably, this right to explanation is applicable unless there is already a stronger or comparable right provided by national or Union law. The GDPR arguably already offers a version of this right for scenarios involving personal data with Recital 71 indicating that individuals should have the ability to request an explanation for automated decisions. Thus, rather than duplicating, the purpose of the Article 86 AI Act is to reinforce and fill in gaps. The AI Act's explanation right steps in to make sure no one is left without recourse in the event that GDPR's Article 22 and related provisions would not cover a specific AI-driven decision for instance, if the decision is not "solely" automated or if personal data is not used, making it fall outside the GDPR.[90]

In any case under either of the two regimes, a person who has been negatively impacted by an automated decision may request transparency and a possible reversal of that decision by using either the AI Act's explanation right or the GDPR's rights to access, objection and human review or even both. Accountability for algorithmic decisions is significantly increased by this coordinated web of rights. It implies that an AI cannot just "decide and forget" and instead its choices are subject to scrutiny and need to be justified to the individuals that they affect. The AI Act's "right to an explanation" aligns with GDPR's transparency objectives which ensures individuals affected by high-risk AI decisions are not left in the dark. This convergence is crucial for operationalizing algorithmic accountability and protecting rights and to create a legal baseline for contesting opaque or potentially discriminatory algorithmic outcomes.

[89] AI Act, art 86.
[90] Luca Nannini, 'Habemus a Right to an Explanation: so What? – A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act' (2024) 7(1) Proceedings of the Seventh AAAI/ACM Conference on AI, Ethics, and Society (AIES-24), 5 – 6 <https://doi.org/10.1609/aies.v7i1.31700> accessed 10 April 2025.

3.4.2. Fairness in High Risk Applications

Finally, both instruments ask for special attention when it comes to profiling and sensitive data, recognizing the impact they can have due to the higher risk. The GDPR strictly regulates profiling involving special categories of personal data which can be the racial or ethnic origin, health, etc. It generally prohibits it unless an exception[91] applies and additional safeguards are in place.[92] The AI Act similarly acknowledges that sometimes sensitive personal data might be processed to mitigate bias in AI to, for example, test an AI system for gender or racial bias as one might need to use data on those attributes. The AI Act addresses this by limiting the processing of special-category data for high-risk AI training or testing to strictly controlled conditions, essentially requiring that it satisfies a significant public interest exception under GDPR and that the proper safeguards are implemented.[93]
Recital 69 of the AI Act clarifies that providers should use sensitive data for bias monitoring or correction only if it is strictly necessary and in compliance with Article 9 GDPR which permits such processing as a matter of substantial public interest when there are suitable measures in place. This altogether shows the legal interconnection. While the AI Act addresses the context of bias mitigation unique to AI, it still submits to GDPR's standards on sensitive data. Together, they ensure that especially traits for profiling like ethnicity, political views or biometrics cannot be deployed in AI systems without satisfying both sets of norms. The processing needs to be lawful and justified under GDPR and the AI's use of such data must be obvious to serve to protect individuals under the AI Act's purpose. So, if an AI system were to engage in forbidden discriminatory profiling like a "resume-screening AI" that profiles candidates by gender or religion in a way that contravenes equality and fairness, this then would violate the AI Act's requirement to avoid bias and contradict the GDPR's principles of fairness and non-discrimination subjecting the offender to penalties under both laws.

Concludingly, the GDPR and AI Act interconnect in some ways to protect individuals from unfair or opaque algorithmic treatment. Individual rights and restrictions on automated decisions and profiling are established by the GDPR which also requires human-centric algorithm governance. The AI Act places systemic obligations on those developing and

[91] GDPR, art 9(2).
[92] GDPR, art 22(3) and rec (71).
[93] Marvin van Bekkum and Frederik Zuiderveen Borgesius,'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?'(2023) 48 Computer Law & Security Review 105770, 3 – 6 <https://doi.org/10.1016/j.clsr.2022.105770> accessed 12 April 2025.

implementing AI, requiring them to develop systems that adhere to the same values of transparency, fairness and human supervision. The two instruments guarantee a cohesive protective framework by mutually reinforcing these rules: people are protected both by design (by requiring AI systems to be developed and used in a way that respects human decision-making and avoids discriminatory outcomes) and "after-the-fact" (by rights to information, explanation and human review). This dual approach greatly reduces the risk of unchecked AI-driven harm upholding the core European value that automation must never be an excuse to compromise fundamental rights. Fairness in high-risk AI systems ultimately rests on the integrity of the data and governance procedures that support these technologies, in addition to rights-based prohibitions. The following section therefore turns to the technical backbone of trustworthy AI: data quality, governance, and compliance processes.

3.5. Data Quality, Governance and Technical Alignment

The GDPR and the AI Act strongly align the high standards for data governance and quality. The GDPR has its data quality principles stating that personal data must be "accurate and, where necessary, kept up to date" and any inaccurate data needs be corrected or deleted without any delay. It also mandates data be "adequate, relevant and limited to what is necessary" for the purpose and collected for "specified, explicit and legitimate purposes".[94] These principles ensure that a high data quality is maintained which is essential for the protection of individuals from harm which can come from incorrect or misused data.

The AI Act stresses the same concepts to make sure that AI systems, especially high-risk ones, are trained on and work with good, well-governed data. The AI Act sets detailed requirements for data governance. Datasets for training, validation and testing have to be relevant, representative and as free of errors as possible and must have appropriate statistical properties to avoid bias.[95] This goes with the GDPR's accuracy and data quality mandates but adapts them to the AI lifecycle. Therefore, if an AI system is used to make decisions about individuals, the AI Act needs the data that the system is working with to be sufficiently representative of the population to prevent biased outcomes which then could unfairly disadvantage protected groups.[96] In GDPR terms, this is an extension of the fairness principle which ensures that data-driven inferences do not perpetuate inaccuracies or discrimination. Data controllers having to correct factors which result in inaccuracies in

[94] GDPR, art 5(1).
[95] AI Act, art 10(3).
[96] Marvin van Bekkum,'Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act' (2025) 56 Computer Law & Security Review 106115, 4 – 9 <https://doi.org/10.1016/j.clsr.2025.106115> accessed 12 April 2025.

profiling and prevent discriminatory effects on the basis of sensitive attributes is indeed mentioned in the GDPR.[97] This gets operationalized in the AI Act with developers being required to, as previously mentioned, actively monitor and curate their datasets to reduce bias and inaccuracy which essentially incorporates GDPR's data quality values into the AI development process.

3.5.1. Governance Processes

Both laws also stress the importance of governance processes around data. GDPR compliance requires organizational measures like data inventories, documentation of processing activities and assignment of responsibility to monitor data use.[98] Correspondingly, the AI Act requires that providers of high-risk AI implement data governance practices as part of their risk management. This includes assessments of provenance and quality of data as well as keeping records of data usage and preprocessing steps.[99] Actually, the AI Act explicitly references the GDPR's governance framework as it notes that in order to facilitate compliance with the EU's data protection law, data governance practices for AI "should include, in the case of personal data, transparency about the original purpose of the data collection".[100] This reference to "original purpose" is significant as it invokes GDPR's purpose limitation principle which is, for example, if personal data that was collected for one reason and later reused to train an AI model. Here, the AI Act expects transparency about that repurposing and needs to reuse to be lawful under the GDPR which would typically require compatibility with the original purpose or a new legal basis. Thus, an AI developer cannot escape the GDPR's orbit and has to manage their training data in a way that respects how and why the data was initially gathered.[101]

The two laws stress continuity of data governance from collection to algorithm ensuring that data does not lose its legal and ethical protections just because it enters a training dataset. One thing is clear, if an AI system uses personal data it should use no more data than necessary and should integrate privacy features from the outset just as asked for in Article 25 GDPR. While the AI Act focuses on broader risks, it implicitly supports these principles for example by encouraging use of privacy-enhancing techniques in AI model training and

[97] GDPR, rec (71).
[98] GDPR, art 30.
[99] AI Act, art 10(2).
[100] AI Act, rec (67).
[101] ibid.

testing.[102] Together they promote robust data hygiene with data inputs needing to be limited to what is needed, relevant to the task, lawfully obtained and continuously checked for quality and bias.

3.5.2. Data Quality

Quality of data is also linked to broader accountability and certification under both laws. The GDPR allows the establishment of data protection certification mechanisms to prove compliance to processing operations standards.[103] The AI Act then also mandates conformity assessments for high-risk AI systems, comprising the evaluation of AI datasets and data governance practices.[104] A significant concern could therefore be the interaction between the two certification systems. The EDPB has emphasised the necessity to clarify the relationship between AI system certification and GDPR compliance certification ensuring that an AI's CE mark[105] does not automatically signify adherence to data protection regulations.[106] Ideally, the processes will be synchronised as an AI system handling personal data should not obtain its AI Act compliance evaluation unless it simultaneously adheres to GDPR's data stipulations for instance, if sensitive data is used, the assessor must verify that a GDPR Article 9 exception is applicable.

The AI Act progresses in this direction by mandating the participation of data protection specialists in the development of harmonized standards for AI.[107] In practice, this implies that data quality assessments under the AI Act, such as ensuring that a training dataset is free of prohibited bias, will inherently incorporate GDPR evaluations like verifying that the dataset does not unlawfully contain personal data collected without consent. The alignment of standards is beneficial for practitioners: adherence to GDPR principles of accuracy, relevance and storage limitations instantly supports compliance with the AI Act's requirements for data set quality and governance.[108] So for example, if a company implemented GDPR measures to continually update or delete no longer relevant personal data, any AI models developed using that data will inherently use more accurate and up to

[102] ibid.
[103] GDPR, Art 43.
[104] ibid.
[105] AI Act, rec (129).
[106] n 55, 3.
[107] AI Act, rec (67).
[108] Eva Thelisson and Himanshu Verma, 'Conformity assessment under the EU AI act general approach' (2024) 4 AI Ethics, 117 and 118 < https://doi.org/10.1007/s43681-023-00402-5> accessed 14 April 2025.

date information, thereby diminishing the likelihood of AI inaccuracies and thus fulfilling the AI Act's requirement for optimal accuracy of data.

An important GDPR-related principle relevant to AI systems is the Right to be Forgotten (RTBF) which was first recognized by the CJEU in its landmark judgment *Google Spain SL and Google Inc. v AEPD and Mario Costeja González*.[109] This case established that individuals have the right to request the removal of outdated, irrelevant or excessive personal information from search engine results which layed the foundation for Article 17 GDPR.[110] Conceptually, the RTBF protects privacy and autonomy, reflecting Europe's commitment to human dignity and informational self-determination, principles which are particularly relevant in an AI-driven world where personal data can be deeply embedded into algorithmic systems. [111]

However, with the rise of AI there are significant challenges to the practical enforcement of the RTBF. Unlike search engines, AI systems do not only index data but internalize patterns especially those based on machine learning. Once personal data is used to train a model it becomes rather difficult or even impossible to erase its influence without retraining the model entirely. Techniques like algorithmic unlearning are being explored but remain in early stages and are difficult to scale. Later CJEU rulings as for example *GC and Others v CNIL* which discussed the balance between privacy and freedom of information, show that even in traditional internet contexts the RTBF requires careful balancing.[112] These tensions are exacerbated by AI which makes it significantly more difficult to ensure individual rights while maintaining system functionality and justice. Determining whether training data is still "personal" presents another challenge. Data must be considered personal if re-identification is reasonably likely as per the CJEU's *Breyer* ruling,[113] which is something that gets harder to determine as AI methods advance

Overall, there are significant legal and technical conflicts when applying the RTBF to AI systems. The realities of machine learning, where data is converted into irreversible abstractions, conflict with traditional privacy rights which are based on the notion of

[109] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317.
[110] ibid, para 88.
[111] Pia Friederike Bettelhäuser, 'AI & the Right to be Forgotten under the GDPR' (Master Thesis, Lund University 2022), 30 – 32 <http://lup.lub.lu.se/student-papers/record/9082521> accessed 11 April 2025.
[112] Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:773, para 66.
[113] C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 48.

removable and traceable data. It will take both technology advancements to make AI more privacy-preserving from the start and clearer regulatory frameworks on concepts like algorithmic unlearning to close this gap.[114]

3.5.3. Data Security and Integrity

Another area of overlap concerns the security and integrity of data. The GDPR asks for appropriate security measures for personal data to protect against any unauthorized modification or loss as breaches may impact data integrity or lead to biased outcomes.[115] The AI Act then similarly requires that high-risk AI systems be resilient against manipulation and errors which includes the integrity of training and input data. A compromised or tainted dataset can lead to inconsistent AI performance and preventing this is equally a matter of data governance as of cybersecurity.[116] Consequently, upholding data quality under the AI Act entails data security which strengthens the GDPR's stipulations. The two laws compel organizations to adopt robust data management frameworks. An organization that has identified its data flows, established access controls and documented its data lineage for GDPR purposes can be adequately equipped to provide proof under the AI Act of how its AI training data was sourced, filtered and secured. Furthermore, data retention is regulated in both frameworks as the GDPR's principle of storage limitation stipulates that data must not be retained longer than necessary[117] while the AI Act mandates that logs and datasets for high-risk AI be kept for a particular period to allow for traceability without prejudice to the GDPR's rules.[118]

Striking a balance between storing sufficient data for auditability and avoiding excessive data retention that infringes on privacy will be integral to the joint compliance exercise, possibly guided by further regulatory and EDPB guidance. Ultimately, the alignment between the GDPR and the AI Act regarding data security and integrity shows the necessity of a holistic compliance strategy. By addressing vulnerabilities in data governance and ensuring traceability, these frameworks collectively promote secure, reliable and ethical AI

[114] n 104, 41 – 49.
[115] GDPR, arts 5(1)(f) and 32; Sylwia Kosznik-Biernacka, 'The Analysis of Risks to Personal Data Security' (2020) 34(34) Security Dimensions 256, 258 and 259 < DOI 10.5604/01.3001.0014.5614> accessed 10 April 2025.
[116] Ronan Hamon, Henrik Junklewitz and Igancio Sanchez, 'Robustness and Explainability of Artificial Intelligence' (*Publications Office of the European Union,* 2020) 10 <doi:10.2760/57493> accessed 15 April 2025.
[117] GDPR, art 5.
[118] AI Act, rec (69).

deployment. They reaffirm that effective AI regulation begins with high-quality and secure data.

3.6. Conclusion

The interplay between the GDPR and the AI Act shows a strategic and carefully coordinated effort by the EU to develop a robust, rights-based framework for the regulation of data-driven technologies. Even if they are different in scope and application with the GDPR focusing on personal data protection and the AI Act on the safety and trustworthiness of AI, they both converge in their underlying principles and operational mechanisms. They both share a foundational commitment to upholding fundamental rights especially privacy, non-discrimination, human dignity and autonomy and apply risk-based, principle-driven approaches that adapt to the complexity and evolving nature of digital innovation.

Throughout this chapter it has been shown that the GDPR and the AI Act are not isolated tools but rather complementary in a broader regulatory system. Together, they create a layered system in which personal data used in AI systems is protected not only by the GDPR's strict requirements on data processing but also by the AI Act's focus on systemic safeguards such as risk management, transparency and explainability. Mechanisms like DPIAs and FRIAs show how they reinforce one another and encourage both anticipatory governance and post-deployment accountability.

Moreover, they align beyond rights protection into shared obligations regarding data governance, documentation, oversight and enforcement. Organizations working with high-risk AI systems have to follow both sets of requirements which means that compliance with one regulation often supports or necessitates compliance with the other. This integrated approach encourages a culture of responsible innovation where ethical considerations are embedded into the design, development and deployment of AI. Significantly, both laws recognize the risks to individuals and society that automated decision-making and profiling can pose if those systems are not being checked. By having mutually reinforcing safeguards like the right to human intervention, transparency about algorithmic processes and restrictions on sensitive data use, the GDPR and the AI Act together aim to ensure that algorithmic systems do not undermine democratic values or human rights.

In conclusion, while the GDPR and the AI Act were drafted in response to different technological and regulatory challenges, they are united by a common goal which is to ensure that technological progress serves people and not the other way around. Their points

of alignment lay the groundwork for a future in which AI and data use are governed by coherent, enforceable and ethically grounded standards which makes the EU a global frontrunner in shaping trustworthy digital governance. While the foregoing chapter highlighted the many areas of convergence between the GDPR and the AI Act, full alignment is not sure. In practice, overlapping mandates, conceptual tensions and enforcement gaps challenge the effective co-application of both frameworks. Chapter 4 therefore addresses the most pressing legal conflicts at the intersection of AI and data protection law.

4. Legal Frictions Between the GDPR and the AI Act

As mentioned the GDPR and the AI Act are two pillars formed by the EU to approach digital technology regulation with the GDPR protecting personal data and privacy as fundamental rights and the AI Act creating a horizontal framework for trustworthy AI with its strict rules for high risk systems. Both regimes are overlapping when it comes to the processing of personal data, in fact the AI Act states that there is no prejudice to the GDPR as they work complementary which means that there must be compliance with both sets of obligations.[119]

Of course, this is deliberate as the AI Act seemingly was drafted drafted on the same EU Treaty basis as the GDPR,[120] showing that many AI risks are also data protection risks. However, having to comply to both laws simultaneously can raise complex legal tensions. Data Protection Authorities have already enforced GDPR against AI uses when there were no AI-specific laws.[121] This was done on grounds of on lack of legal basis, opacity in algorithms or automated decision-making abuses.[122] The AI Act adds additional requirements which must connect with the GDPR's existing mandates, especially for high-risk AI applications like credit scoring, biometric identification or AI in recruitment.

[119] AI Act, rec (9).
[120] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/1 (hereinafter TFEU), art 16.
[121] e.g. "Italian DPA's temporary ban decision on OpenAI's ChatGPT, the Italian DPA's Deliveroo fine in relation to the company's AI-enabled automated rating of rider performance, the French DPA's Clearview AI fine, a facial recognition platform that scrapes billions of photographs from the internet and the Dutch DPA's fine on the Dutch Tax and Customs Administration for various GDPR infringements in relation to an AI-based fraud notification facility application" in James Clark, Muhammed Demircan and Kalyna Kettas, 'Europe: The EU AI Act's relationship with data protection law: key takeaways' (*DLA PIPER*, 25 April 2024) <https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/> accessed 31 March 2025.
[122] ibid.

This chapter shall explain the following key challenges at the GDPR–AI Act intersection for high-risk AI systems: (1) transparency and explainability of AI decisions, (2) automated decision-making and the right to human oversight, (3) the legal basis for AI data processing, (4) bias, discrimination and data protection risks and (5) enforcement and regulatory overlaps. Each section identifies core legal tensions, ambiguities as well as practical challenges when trying to satisfy both regimes. This shall be supported by relevant case law, regulatory opinions and commentary. The overarching theme is the interplay between fundamental rights and emerging AI governance as high-risk AI systems can put rights at risk but also bring great benefits, testing how GDPR and the AI Act can work together to ensure accountability. CJEU rulings show the increasing complexities and challenges emerging at this intersection especially when it comes to transparency, automated decision-making, legal bases for data processing, bias and enforcement.

4.1. The Challenge of AI Transparency and Explainability

Even if there is no universally accepted legal or ethical definition of AI explainability, transparency and explainability remain central concerns. The European Commission's High-Level Expert Group on AI describes explainability[123] as fundamental to fostering user trust. According to their definition, explainability is about making sure that processes are transparent, the capabilities and purposes of AI systems are clearly communicated and that the outcomes of AI-driven decisions can be explained to those affected. [124] Such transparency is crucial as decisions must be able to get challenged.

However, to achieve full explainability can be difficult or even impossible particularly for complex models such as "black box" algorithms. In such cases, the Expert Group suggests alternative forms of explicability including traceability, auditability and open communication about the system's capabilities.[125] These alternatives must still be enough to guarantee that AI systems respect fundamental rights even when full insight into their internal logic is not feasible. The required level and form of explainability thus really

[123] or explicability as mentioned in the report.
[124] 'Ethics Guidelines for trustworthy AI' (*European Commission*, 8 April 2019) 13 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 15 April 2025.
[125] ibid 20 – 24.

depends on the context of the AI application especially in terms of the severity and consequences of potential errors. [126]

Explainability also goes beyond just technical transparency as it involves understanding both how AI systems function and also how human choices shape their deployment. Even though technical explainability allows users to trace how decisions are made, it often involves trade-offs. Higher explainability can reduce a system's complexity and thereby accuracy, whereas highly accurate systems then may be less transparent. Therefore, explainability duties should be proportionate to the impact of decisions on individuals and tailored to stakeholders' levels of technical understanding.[127]

To ensure transparency in business activities, organizations must document how AI systems influence decisions, design and deployment. The GDPR requires transparency in data processing, notably through the right to information and provisions on automated decision-making. Article 22 GDPR gives individuals the right not to be subject to decisions with significant legal effects which are solely automated. In the *SCHUFA Holding (Scoring)* case, the importance of informing individuals about the logic behind algorithmic credit scores was emphasized and thereby reaffirmed their right to contest such decisions which reinforces Article 22 and supports the AI Act's focus on human oversight in high-risk AI systems.[128] With that the GDPR gives individuals the explicit right to understand the scope and purpose of data processing and data controllers have to provide this information transparently and intelligibly using clear language.[129] Beyond protecting data, the GDPR aims to safeguard fundamental rights in the face of technological change. While Article 22 does not provide a standalone "right to explanation" it strengthens the concept indirectly by demanding meaningful information about automated decisions.[130] Recital 71 affirms the right to challenge such decisions and get explanation which has sparked academic debate, with some denying a distinct right to explanation, while others stress its practical importance in giving

[126] Alexandre de Streel, Adrien Bibal, Benoit Frenay and Michael Lognoul, 'Explaining the Black Box: when law controls AI' (*cerre Centre on Regulation Europe*, 3 February 2020) 4 <https://cerre.eu/wp-content/uploads/2020/03/issue_paper_explaining_the_black_box_when_law_controls_ai.pdf> accessed 21 April 2025.
[127] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 65, 88 – 92 <https://doi.org/10.1080/13600834.2019.1573501> accessed 21 April 2025.
[128] Case C-634/21 *OQ v Land Hessen* [2023] ECLI:EU:C:2023:957, paras 56 and 57.
[129] GDPR, art. 12(1).
[130] GDPR, art 15(1)(h).

individuals the possibility to contest and verify algorithmic decisions.[131] Ultimately, the goal is to uphold fairness and access to justice which includes the right to a fair trial.

Crucially, only decisions that have a significant effect on individuals are covered by Article 22 GDPR. Since even routine digital services like price comparison tools can have a significant impact on users, some argue for broader application. Clarity regarding algorithmic logic is necessary to provide meaningful explanations which can be challenging when facing complex models. The continuous debate emphasizes the necessity of fair, situation-specific transparency measures that protect rights while supporting innovation.[132]

A major challenge in aligning the GDPR and the AI Act lies in ensuring explainability of AI-driven decisions. As described before, the GDPR mandates that individuals be informed clearly and accessibly about personal data processing[133] which can get more complex when it comes to AI especially in machine learning "black boxes" which are inherently opaque, complicating these obligations and creating legal uncertainty. This is particularly relevant under large generative AI models such as ChatGPT which raise broader transparency concerns. Under Articles 13 and 14 GDPR, providers must explain how the data is gathered and then used. Article 13 applies when data is collected directly from users, while Article 14 covers situations where data is gathered indirectly as for example through training datasets. While informing users about the data they directly provide is rather simple, meeting the obligations regarding vast, unstructured datasets under Article 14 is substantially more difficult. Under Article 14(5)(b), controllers may invoke the "disproportionate effort" exemption but they are still required to put safeguards in place to protect the rights of individuals. The GDPR implicitly calls for a balance between the effort required to inform and individuals' right to be informed. The majority of AI-related processing, however, does not clearly fit into exemption categories like statistical or scientific use. Furthermore, AI models' opacity makes them more vulnerable to "inversion attacks" in which training data is reconstructed, posing significant privacy risks. Here, authorities could enhance legal certainty and compliance by providing clearer guidance.[134] Transparency is essential not

[131] Michelle Miao, 'Debating the Right to Explanation: An Autonomy-Based Analytical Framework' (2022) 34 Singapore Academy of Law Journal 864, 870 and 871 <https://dx.doi.org/10.2139/ssrn.4225103> accessed 25 April 2025.
[132] Jarek Gryz and Marcin Rojszczak, 'Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem' (2021) 10(2) Internet Policy Review, 3 – 5 <https://doi.org/10.14763/2021.2.1564> accessed 25 April 2025.
[133] GDPR, arts 12 – 14.
[134] Philipp Hacker, Johann Cordes and Janina Rochon, 'Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection

only for the safekeeping of rights but also for ensuring fairness, accountability and public trust in AI systems. Without any or reduced transparency, individuals may lose control over their data and face discrimination following opaque decisions. Clear explanations help with identifying and correcting bias and errors as well as with data protection and anti-discrimination compliance. The GDPR indirectly addresses the corresponding challenges by requiring "meaningful information about the logic involved" under Article 15(1)(h) supported by Recital 71. Yet fulfilling these obligations can be difficult especially in cases with complex AI systems. The AI Act addresses this by imposing the previously discussed specific duties on providers of high-risk systems to ensure transparency with documentation and oversight. However, there still is a gap between the GDPR's emphasis on user comprehensibility and the AI Act's technical transparency requirements.[135]

Regulators and organizations must close this gap and guarantee coherent protection to then build a sustainable, accountable AI governance framework requires striking a balance between innovation, individual rights and public trust. Explainability and transparency are of utmost importance for user trust but they must be supported by solid human control over AI systems. The next section explores how the GDPR and AI Act operationalize human oversight especially regarding automated decision-making.

4.2. Human Oversight in Automated Decision-Making

Individuals are explicitly protected from decisions based solely on automated processing under the GDPR especially when these decisions have significant legal or similarly substantial effects. Such decisions usually include hiring outcomes, credit assessments or law enforcement profiling.[136] This makes sure that affected individuals have the right to request human intervention, contest the decision and get clear explanations about how the decision was reached. In comparison, the AI Act highlights the importance of human oversight especially when it comes to high-risk AI systems but does not categorically prohibit fully automated decision-making, unlike the GDPR.[137] This distinction could potentially create regulatory tension and cause uncertainty among businesses and public authorities regarding their legal obligations with respect to human involvement in AI-driven

Regulation and Beyond' (2023) 15(1) European Journal of Risk Regulation 49, 60 <https://doi.org/10.1017/err.2023.81> accessed 25 April 2025.

[135] Chinara Gasimova, 'Privacy and Transparency in an AI-driven World: Does Algorithmic Transparency Fit on Data Privacy Under GDPR?' (Master Thesis, Lund University 2023), 32 – 43 <http://lup.lub.lu.se/student-papers/record/9119730> accessed 26 April 2025.

[136] GDPR, art 22(1).

[137] AI Act, rec (10).

decisions. The *SCHUFA Holding (Scoring)* judgment reinforced the necessity of providing individuals with information about the logic involved and offering them meaningful opportunities for human intervention which shall ensure that AI-driven systems, especially high-risk ones, do not make unchecked decisions affecting individuals' rights.[138]

The primary reason for the overlap between these two frameworks is that automated decision-making (ADM) procedures, especially those that involve profiling, are directly covered by Article 22 GDPR. As a consequence it was necessary to evaluate the EU's regulatory initiatives on AI in connection with GDPR provisions. In their communication on human-centric AI, the European Commission underscored the necessity of human supervision in the development and deployment of high-risk AI systems which aligns with the GDPR's overarching objectives of preserving individual autonomy and ensuring transparency.[139] Initially, these documents explicitly pushed the concept of "human-centric AI" which continues to significantly influence the Act's essence even if it is not explicitly addressed in the subsequent AI Act proposal from 2021.[140] As stated in the Articles 8(1) and 14, the AI Act makes it clear that high-risk AI systems must be under human oversight. Notably, the AI Act takes the GDPR's monitoring principles beyond the user stage and includes protections and ways to oversee during the AI system's design and development phases.

In line with the AI Act, the lifecycle of AI systems is divided into two principal stages: the development phase which involves "providers" and the usage phase which concerns "users". The AI Act proactively incorporates human oversight mechanisms from the very beginning of AI development whereas the GDPR focusses on oversight obligations in the usage stage. Recital 48 of the AI Act Proposal (Recital 73 of the final AI Act) mandates that providers design high-risk AI systems in a way that enables effective human oversight from the earliest stages of development. These oversight measures have to ensure responsiveness to human operators who must have sufficient training, competence and authority and also need to have built-in operational constraints that the AI system itself cannot override. The AI Act goes into further detail about the providers' responsibilities from Article 8. By designing AI systems which can be efficiently monitored by people

[138] n 121.
[139] Commission, 'Communication: Building Trust in Human Centric Artificial Intelligence' COM(2019) 168 final, 4.
[140] Celso Cancela-Outeda, 'The EU's AI act: A framework for collaborative governance' (2024) 27(3) Internet of Things 101291, 4 – 6 <https://doi.org/10.1016/j.iot.2024.101291> accessed 22 March 2025.

while in operation, providers can ensure adherence to human oversight standards.[141] Before entering the market, providers must either explicitly explain and inform users of the necessary oversight mechanisms or incorporate these measures within the AI system itself if possible.[142] By giving human overseers the ability to correctly understand the system's capabilities and limitations, appropriately interpret its outputs and stop or adjust system activities when necessary, such measures empower them.[143] Also, the AI Act sets transparency requirements in Article 13 which make these oversight measures even stronger by making sure that information about the AI system's functions and limits is clear and accessible. Users of AI are obliged by Article 29 to make effective use of the oversight information given by system developers which shows a deliberate and thorough attempt to harmonize the AI Act with GDPR obligations since it supports and aligns with users compliance with the Data Protection Impact Assessment requirement under Article 35 of the GDPR.[144]

The AI Act's emphasizing human oversight represents a major improvement over previous regulatory frameworks especially the European Commission's White Paper on AI.[145] Transparency and accountability are reinforced by the transition from the White Paper to the official AI Act proposal which shows a stronger commitment to legally ensuring human oversight at every level of AI deployment. The AI Act reduces potential biases and inaccuracies in automated decision-making and ensures compliance with GDPR standards by requiring explicit oversight and documentation requirements early in the design and development stages thereby strengthening the protection of individuals' rights. [146]

Even if the need for human oversight shows the importance of procedural safety measure there still remains the question about a more fundamental issue which is on what grounds an AI system can lawfully process the vast amount of data it relies on. The next section will adress this critical question by examining the legal bases for data processing under the GDPR in the context of AI. Even though human oversight ensures procedural safeguards, there exists another fundamental challenge in the very legal justification for processing personal

[141] AI Act, art 14(1) and 16(a).
[142] AI Act, art 14(2).
[143] AI Act, art 14(4).
[144] Guillermo Lazcoz and Paul de Hert, 'Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities' (2023) 50 Computer Law & Security Review 105833, 6 – 7 <https://doi.org/10.1016/j.clsr.2023.105833> accessed 12 April 2025.
[145] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final.
[146] n 142.

data in AI systems. The next section addresses the foundational question on how personal data can be lawfully in the AI lifecycle.

4.3. Legal Bases for Personal Data Use in AI Systems

AI systems usually rely on big sets of data for training and optimization which raises questions concerning the legal foundation for data processing under the GDPR. Any act of data processing under Article 6 which describes justified grounds including consent, legitimate interest or contractual necessity, has to be justified under the regulation. On the other hand, AI applications that repurpose or reuse data outside the initial scope of consent could potentially breach GDPR's purpose limitation principle.[147]

While the AI Act establishes requirements for data governance and quality,[148] it does not give any legal guidance on how AI developers should balance these requirements with the GDPR's constraints. AI-driven businesses could find it difficult to navigate compliance requirements due to this regulatory gap. The interplay between the GDPR and AI Act creates complex legal challenges especially when it comes to justifying the processing of personal data in AI-driven settings. The principle of purpose limitation under the GDPR Article 5(1)(b) states that information that was originally gathered for one specific purpose must not be used again for any other purpose unless the subsequent use corresponds to the original intent. This principle is particularly challenging for AI systems as machine learning models frequently depend on large datasets originally collected for unrelated purposes. The regulatory ambiguity becomes especially challenging when looking at the different phases of AI data processing each of which may implicate different legal bases under the GDPR. AI data processing typically includes five separate phases: the collection of training data, the processing of data for AI training, the provision of AI applications, the use of those applications and the utilization of AI-generated outputs. Each of these stages can potentially involve the handling of personal data and therefore requires its own lawful justification.[149]

Obtaining training data can involve getting personal information from self-collected means like sensors or cameras or publicly accessible online content. Once gathered, this data is used for the initial training and the later fine-tuning of AI models. When an AI application gets

[147] 'Handbook on European data protection law' (*Publications Office of the European Union,* 2018), 122 <doi:10.2811/343461> accessed 25 April 2025.
[148] AI Act, art 10.
[149] Nicole Kopp, 'Legal bases for data processing by AI' (*activeMind.legal*, 30 September 2024) <https://www.activemind.legal/guides/legal-bases-ai/> accessed 15 April 2025.

available, the system may continue processing personal data either from its original training dataset or from new user inputs. Furthermore, the AI's outputs may themselves contain or be used to infer personal data which potentially triggers additional data protection obligations especially when combined with other datasets. In determining the appropriate legal basis under Article 6 GDPR for each processing phase, there theoretically are several options are available. These options include consent, contractual necessity, compliance with a legal obligation, protection of interests, performance of a task carried out in the public interest or official authority as well as legitimate interests by the data controller.[150] However, as relying on legitimate interests is particularly difficult to justify given the opaque and potentially intrusive nature of many AI systems it can be difficult to put this into practice in the AI context. Although consent is frequently regarded as the most reliable option, it must be specific, revocable, informed and freely given, all of which can be challenging to achieve in large-scale or non-transparent AI deployments. The GDPR's definition of consent in Article 4(11) and outlined Article 6(1)(a) introduces a great deal of complexity to AI contexts as it must be clear, informed, freely provided and easily revocable.[151] It is especially difficult to ensure truly informed consent because of the complexity, opacity and dynamic nature of AI systems. The practicality of consent as a legal foundation for AI-based processing is severely limited by the EDPB Guidelines 05/2020 which make it clear that generalised or vague consents are insufficient to meet the GDPR's standards.[152]

Legitimate interests under Article 6(1)(f) GDPR form an alternative legal basis although subject to a strict balancing test that carefully weighs the data controller's interests against the rights and freedoms of the concerned data subjects. The inherent opacity, unpredictability and potential extensive profiling capabilities of AI systems make this balancing exercise rather complicated. ECJ jurisprudence, as for example the mentioned *Breyer* as well as *Google Spain* cases, underscore the importance of comprehensive transparency, rigorous documentation and robust protective measures which increases the compliance burden for AI developers.

The contractual necessity basis provided by Article 6(1)(b) GDPR is similarly restrictive and applies only where data processing is directly essential for the execution of a contract. The

[150] GDPR, art 6(1).
[151] GDPR, art 7.
[152] Guidelines 05/2020 on consent under Regulation 2016/679 adopted on 4 May 2020 [2020], 14 <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf f> accessed 28 April 2025.

EDPB Guidelines advise against overly broad interpretations of contractual necessity especially when it comes to activities that just enhance services rather than being integral to contractual obligations.[153] Consequently, many AI applications could fail to satisfy this legal justification.

Increasing the complexity, the AI Act introduces explicit requirements around data quality, governance, transparency and risk management.[154] However, it lacks clear guidance on alignment with GDPR principles such as data minimization and purpose limitation and this regulatory ambiguity could be significant source of uncertainty, complicating compliance and potentially limiting innovation due to overly cautious interpretations aimed at minimizing regulatory risks.

Article 6(4) GDPR provides possibilities for secondary data processing, contingent upon satisfying the compatibility test emphasizing transparency, fairness and accountability. For AI such secondary uses like model training and algorithm optimization, may be permissible if supported by strong transparency measures and protective safeguards that adequately respect the data subjects' rights. Furthermore, the processing of special categories of personal data like biometric or health data, has higher requirements[155] and systems that are working with such sensitive data must meet strict standards of explicit consent or substantial public interest justification which shall ensure necessity, proportionality and stringent safeguards.[156] The ECJ has emphasized the strict standards needed for explicit consent in these sensitive contexts by the requirement of meticulous compliance frameworks. Recent ECJ jurisprudence, *Meta Platforms Ireland*[157] and *Orange Romania* (C-61/19)[158] in particular, show an increasingly strict interpretation of GDPR's legal bases focusing on transparency, specificity in consent and contractual clarity. AI developers must proactively adopt strict compliance strategies in line with the evolving regulatory expectations as these rulings show increased judicial scrutiny of AI-driven data processing. When AI processing

[153] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects [2019], 14 <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 28 April 2025.
[154] AI Act, arts 10 – 11.
[155] GDPR, art 9.
[156] Nicole Kopp, 'Legal bases for data processing by AI' (*activeMind.legal*, 30 September 2024) <https://www.activemind.legal/guides/legal-bases-ai/> accessed 15 April 2025.
[157]Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, paras 73, 85, 126 and 154.
[158] C-61/19 *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* [2020] ECLI:EU:C:2020:901, para 52.

presents a significant risk to individual freedoms and rights, a proactive and cautious approach is required to address these challenges which can be achieved through DPIAs. Furthermore, it is essential to incorporate the principles of privacy by design and by default into the development and operation of AI systems. Transparency with data subjects is crucial, particularly when it comes to the nature, scope and purpose of processing. In the end, AI developers must ensure that people can effectively exercise their GDPR rights which include the right to erasure, access to their data, and rectification of inaccuracies.

Altogether, these recommendations show how important it is to find a phase-specific and situation-specific way to legally process AI data. Even though the GDPR gives a broad framework, it does not specify much about AI specifically. This is also not covered by the AI Act which makes for little legal certainty. In this environment, ensuring compliance does not only need a careful legal analysis but also the implementation of robust technical and organizational safeguards from the outset of AI system development.

4.4. Discrimination, Bias and Fairness Risks in AI Deployment

The AI Act aims to foster human-centric, trustworthy and sustainable AI which safeguards individuals' fundamental rights, especially data protection. Among its core objectives is the mitigation of discrimination and bias particularly when it comes to high-risk AI systems. This includes provisions to allow the processing of "special categories of personal data" such as race, ethnicity, political opinions, beliefs, trade union membership, genetic data, biometric data, health data or data concerning sexual orientation. This with the aim of strictly detecting and addressing bias. Conflicts between the AI Act's provisions on special data categories and the GDPR's stricter standards, however, could result in legal ambiguities that call for additional legislative or regulatory clarifications. The AI Act acknowledges that identifying discrimination often needs processing exactly such sensitive data like ethnicity or health-related characteristics even though the GDPR generally forbids processing sensitive data unless there is express consent or a compelling public interest. [159]

Under the GDPR, processing sensitive personal data is not allowed unless specific legal requirements are met. These specific grounds can be explicit consented to by the data subject

[159] Marvin van Bekkum,'Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act' (2025) 56 Computer Law & Security Review 106115, 2 <https://doi.org/10.1016/j.clsr.2025.106115> accessed 12 April 2025.

or by a substantial public interest which makes the processing necessary.[160] The AI Act introduces a controlled exception to allow such processing when it is required to identify and mitigate discrimination within AI systems. However, for that robust safeguards such as technical and organizational measures to ensure data security, access restriction and data minimization, need to be put in place.[161] This exception is follows Article 9(2)(g) GDPR which allows processing when supported by Union or Member State law as long as the processing is proportionate, respects the essence of the right to data protection and includes appropriate safeguards for the rights and freedoms of individuals.[162]

When AI systems are trained on large datasets, they have a tendency to replicate and amplify societal biases, either by being in the data itself or by being introduced during algorithmic design and data annotation. Predictive policing tools that may unfairly target specific communities, credit scoring systems that disadvantage certain ethnicities, facial recognition systems that have higher error rates for darker skin tones and recruitment algorithms that disproportionately reject minority candidates are just a few examples of how discrimination can appear.[163] Even generative AI systems like chatbots or AI content creations which may not even be initially classified as high-risk can spread harmful stereotypes, hate speech or misinformation.[164] The AI Act therefor provides the European Commission with the power to update the list of high-risk AI systems in Annex III through delegated acts to make sure that the regulatory framework remains responsive and up to date to emerging threats to fundamental rights.[165]

Bias in AI systems can come from many different sources such as the use of non-representative training data, flawed algorithmic assumptions or subjective human decisions in labeling or feature selection. These systemic issues lead to decision-making errors that can increase structural inequalities even more. To counteract this, the AI Act needs providers of high-risk AI systems to document and analyse their training, validation and testing datasets.[166] Providers have to apply de-biasing strategies, ensure dataset representativeness

---

[160] GDPR, art 9.
[161] AI Act, art 10(5).
[162] Marvin van Bekkum,'Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act' (2025) 56 Computer Law & Security Review 106115, 1 – 3 <https://doi.org/10.1016/j.clsr.2025.106115> accessed 12 April 2025.
[163] Philipp Hacker,'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' (2018) 55(4) Common Market Law Review, 8 and 9 <https://ssrn.com/abstract=3164973> accessed 20 April 2025.
[164] Sam Jackson and JM Berger, 'The Dangers of Generative AI and Extremism' (*Middlebury Institute of International Studies*, 12 December 2023) <https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/dangers-generative-ai-and-extremism> accessed 20 April 2025.
[165] AI Act, art 7.
[166] AI Act, art 10.

and test for impacts. This process not only contributes to fairness but also supports compliance with data governance and quality management obligations in general.[167]

However, these obligations intersect with the GDPR's data minimization principle[168] which requires that personal data collected must be adequate, relevant and limited to what is strictly necessary for the stated purpose.[169]

This idea contradicts the data-intensive practices which are used in the AI sector, where better model performance often linked to larger datasets. The CJEU has ruled in cases like *GC and Others v. CNIL*which reaffirmed that excessive or indefinite data retention,[170] even if it was initially legal, can violate EU law and *Huber v. Germany* where the Court held that storing personal data without necessity violated data protection rules.[171] However, there are challenges for AI development that go along with data minimization. Machine learning models typically require huge and diverse datasets to improve their accuracy which then creates tension between GDPR compliance and the AI sector's "more data, better models" paradigm. Developers must show that personal data is lawfully collected for a clearly defined purpose as processing is strictly limited to what is required and retention policies enforce periodic review and deletion of unnecessary data. To reconcile these competing demands, privacy-preserving technologies like federated learning, synthetic data generation and differential privacy are being explored.[172]

Importantly, discrimination risks are not confined to special categories of data. Attributes such as age, gender, postcode or income level, even though not being explicitly classified as sensitive data under the GDPR, can serve as proxies for protected characteristics and lead to indirect discrimination. Processing such non-sensitive data usually relies to the provisions in Article 6 GDPR particularly legitimate interest or performance of a contract as legal bases. However, algorithms that rely on seemingly neutral criteria have the potential to produce outcomes that disproportionately disadvantage certain groups, thereby raising concerns under EU anti-discrimination law. Fairness in automated decision-making is addressed

---

[167] n 163, 16.

[168] GDPR, art 5(1).

[169] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data [...] [2016] OJ L119/1 (General Data Protection Regulation), art 5(1)(c).

[170] Joined Cases C-136/17 *GC and Others v CNIL* [2019] ECLI:EU:C:2019:773, para 74; see also Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 93.

[171] Case C-524/06 *Huber v Germany* [2008] ECLI:EU:C:2008:724, paras 59 – 68.

[172] Nazish Khalid, Adnan Qayyum, Muhammad Bilal and others, 'Privacy-preserving artificial intelligence in healthcare: Techniques and applications' (2023) 158 Computers in Biology and Medicine 106848, 9ff <https://doi.org/10.1016/j.compbiomed.2023.106848> accessed 20 April 2025.

explicitly in Article 22 GDPR and Recital 71. Data controllers must put safeguards in place when automated decisions can have a substantial impact on individuals, such as when it comes to credit approvals, hiring decisions or access to public benefits. These safeguards include human intervention, the ability for individuals to express their views and challenge decisions as well as transparency measures. Scholars and regulators argue that ignoring bias detection and correction responsibilities violates the fairness and accuracy principles enshrined in GDPR. Article 57(1)(a) tasks national data protection authorities (DPAs) with monitoring and enforcing compliance, including ensuring fairness in automated processing.[173]

Even with these legal provisions, enforcement is still difficult. Many DPAs and regulatory bodies lack the technical expertise, financial resources or legal authority to meaningfully audit complex AI systems. Coherent oversight becomes even more difficult by the fragmented institutional landscape and the overlapping mandates of competition regulators, data protection authorities and AI-specific supervisory bodies. To guarantee the successful implementation of the AI Act and the GDPR, it is essential to invest in technical auditing capabilities, harmonise frameworks and provide clearer regulatory guidance.

In conclusion, there are both opportunities and regulatory challenges at the intersection of data protection laws and anti-discrimination objectives. The AI Act's risk-based, forward-looking framework which provides a big palette of tools to support fairness, accountability, and transparency in the deployment of AI, complements the GDPR's rights-based approach well. However, successful implementation, regulatory cooperation and continuous legal and technical development are necessary for this framework to succeed.

4.5. Overlapping Enforcement and Institutional Fragmentation

Understanding the practical implications of the GDPR and AI Act's regulatory interactions depends heavily on their enforcement frameworks. Although protecting fundamental rights is the objective of both systems and they both use a decentralised enforcement approach with their institutional structure, areas of authority and operational capacity being very different. This section shows how overlapping enforcement mechanisms, fragmented institutional mandates and uneven national capacities contribute to regulatory complexity and legal uncertainty. In doing so, it draws attention to the risks of inconsistent and disjointed

[173] Philipp Hacker,'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law' (2018) 55(4) Common Market Law Review, 29 – 30 <https://ssrn.com/abstract=3164973> accessed 20 April 2025.

application of EU data and AI laws and examines the difficulties in coordinating between state and EU-level oversight bodies.

4.5.1 A Common Foundation with Diverging Structures

An important part of understanding the interplay between the GDPR and the AI Act is in their enforcement structures and their regulatory implications. Both aim to safeguard fundamental rights within the EU legal order while addressing technological challenges: personal data processing in the case of the GDPR and the broader regulation of artificial intelligence in the AI Act. Despite their different scopes their enforcement strategies reveal some similarities particularly in their reliance on a predominantly decentralized enforcement model.

Under the GDPR, enforcement is delegated primarily to national Data Protection Authorities (DPAs) and coordinated by the European Data Protection Board (EDPB) which has an advisory and coordinative role without actually having strong enforcement powers.[174] This structure has caused inconsistent decision-making, inconsistent application across Member States and forum-shopping by data controllers looking for more favourable jurisdictions. Furthermore, it has been widely criticised that DPAs differ in their independence, resources and expertise and that certain Member States contradict Article 52 GDPR by underfunding or politically influencing their national authorities. These structural deficiencies have stalled effective enforcement and undermined the credibility and uniformity of the GDPR framework and, by extension, the rule of law in the EU. The AI Act mirrors many of these enforcement patterns by assigning core supervisory and enforcement responsibilities to national competent authorities (NCAs), termed market surveillance authorities (MSAs) for overseeing high-risk and limited-risk AI systems.[175] However, the Act also introduced new centralized elements, notably the European Commission, the AI Office, a scientific expert panel and the European Artificial Intelligence Board (EAIB).[176] These institutions are meant to enhance coordination, oversight and technical expertise,

[174] GDPR, art 68ff.
[175] AI Act, art 70.
[176] AI Act, art 65.

especially in relation to General-Purpose AI (GPAI) systems[177] which are deemed to carry systemic risk. [178]

4.5.2 Fragmentation Risks and Structural Gaps

Despite these mechanisms, enforcement remains decentralized in its core structure and many of the problems seen with the GDPR may recure. One big concern is regulatory fragmentation as different Member States may apply enforcement standards unevenly, especially given varying institutional capacities and national interpretations. This could lead to legal uncertainty for providers, unequal protection levels for individuals and a distorted internal market which mirrors the GDPR criticisms. Also, MSAs, unlike DPAs, are not explicitly guaranteed full independence in the same way which raises concerns about political influence, especially in Member States with weaker democratic safeguards. This is especially critical considering that many AI systems under the AI Act, like remote biometric identification or predictive policing tools, will be deployed by public authorities and thus increasing the risk of state-driven rights infringements without robust independent oversight. Another major issue is the capacity gap. National authorities may not have the technical, financial and human resources to supervise highly complex AI systems effectively. Even with access to EU-level expertise via the scientific panel or advisory forums, enforcement quality could vary dramatically. As was the case under the GDPR, this could weaken compliance incentives for more powerful actors and allow high-risk systems to remain unchecked.[179]

Furthermore, the Commission's increased powers to supervise General Purpose AI (GPAI)[180] and adopt implementing and delegated acts, while a step toward centralization, are limited in scope as they apply only to only a small category of AI systems and not to the majority of high-risk applications which will dominate in the real-world deployment.

---

[177] "General-Purpose AI (GPAI) systems are AI models designed to be versatile and adaptable, capable of performing a wide range of tasks across various applications. They are trained on broad datasets and can be integrated into different downstream systems or applications. GPAI models, like Large Language Models (LLMs), are a key component of many AI systems, including generative AI applications like ChatGPT and Gemini." 'General Purpose AI and the AI Act' (*future of life Institute*, May 2022), 3 <https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf> accessed 21 April 2025.

[178] Kasia Söderlund and Stefan Larsson, 'Enforcement Design Patterns in EU Law: An Analysis of the AI Act' (2024) 3 Digital Society, 10 – 12 <https://link.springer.com/content/pdf/10.1007/s44206-024-00129-8.pdf> accessed 26 April 2025.

[179] ibid, 14 – 15.

[180] «The term 'GPAI' covers an umbrella of AI technologies characterised by "significant generality" and which are "capable of competently performing a wide range of distinct tasks" (Art. 3 AIA), including large-language models (LLMs) and other foundation models. This group of AI technologies have been subjected to closer regulation due to their potential to affect the objectives of the AI Act.» ibid, 10.

Scholars have questioned why a more centralized model, as for example a dedicated European AI agency, was not adopted. This especially when given the AI Act's legal basis in Article 114 TFEU which would allow for stronger central bodies similar to the European Securities and Markets Authority (ESMA).[181]

4.5.3 Jurisdictional Overlap and Coordination Efforts

The enforcement mechanisms of the GDPR and the AI Act vary greatly and may cause jurisdictional conflicts. National DPAs enforce the GDPR through investigations and fines.[182] Then on the other hand, the AI Act creates EU-level coordination systems and national AI authorities to monitor adherence to AI-specific regulations.[183]

The GDPR provides for a two-tier enforcement model with a leading role for DPAs in each Member State which get complemented by the advisory and consistency mechanisms of the EDPB and EDPS. In the absence of AI laws, DPAs were already taking positions on AI as for example the Italian DPA temporarily banned ChatGPT.[184] The AI Act introduces separate terms: "national supervisory authority", "national competent authority", "market surveillance authority" and "notifying authority".[185] These distinctions indicate an attempt to define responsibilities but also raise concerns about overlap and uncertainty.

The AI Act acknowledges the risk of overlap shown by its references to the GDPR and the inclusion of "without prejudice" clauses. These clauses state that the AI Act does not affect the application of EU personal data law, nor the tasks and powers of independent supervisory authorities like the DPAs. However, it still is not exactly clear whether the AI Act constitutes a lex specialis to the GDPR.[186]

Cooperation mechanisms could help to reduce divergences between authorities in EU data law, however specific corresponding rules are lacking. The AI Act suggests that national supervisory authorities should consult competent authorities under EU law, including DPAs, when drafting guidance. At the EU level, the AI Office will include a representative of the EDPS, ensuring that the voice of DPAs is heard, although without decision-making power.

---

[181] ibid, 16.
[182] GDPR, art 51ff.
[183] AI Act, art 64ff.
[184] 'Artificial intelligence: stop to ChatGPT by the Italian SA
Personal data is collected unlawfully, no age verification system is in place for children' (*GPDP Garante per la protezion dei dati personali*, 20 December 2024) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847> accessed 30 April 2025.
[185] AI Act, art 3.
[186] Pawel Hajduk, 'AI Act and GDPR: On the path towards overlap of the enforcement structures' (*RAILS Robotics and AI Law Society*, 1 October 2023) <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/> accessed 30 April 2025.

The AI Office is tasked to support cooperation between national and EU-level authorities including the EDPB and EDPS. However, procedural issues and unclear authority divisions make things more difficult in certain situations. Although this might be deduced from an overall duty to assist public authorities tasked with enforcing fundamental rights, the AI Act does not specifically provide rules for collaboration between national AI authorities and DPAs.[187]

Legal uncertainty and compliance costs are raised through the GDPR and AI Act's overlapping enforcement structures. Given the GDPR's broad definition of personal data and the huge amount of data in AI systems, this challenge highlights a deeper taxonomic issue which lays in the scope of EU data law itself. It will take time and likely some trial and error to resolve this.

4.5.4 Governance and Supervisory Models

In their joint Opinion on the AI Act Proposal the EDPB and EDPS highlight the pre-existing role of DPAs in enforcing the GDPR, the European Union Institutions, Offices, Bodies and Agencies (EUDPR) and the Law Enforcement Directive (LED). This is particularly relevant with regard to AI systems that handle personal data. They argue that DPAs meet the requirements for supervisory positions under the AI Act as they have the necessary expertise of AI technologies, data processing and risk assessment.[188]

The Opinion emphasises that there is a significant overlap with data protection law because many AI systems covered by the AI Act also process personal data so supervisory mandates may overlap or conflict as a result. The EDPB and EDPS advise designating DPAs as national supervisory bodies under the AI Act to address this as this would reduce fragmentation and provide uniform interpretation and enforcement among Member States. Additionally, it would make compliance easier for developers and deployers along the AI value chain by establishing a single supervisory contact point for AI systems involving personal data. The Opinion further emphasises the necessity of independent oversight under Article 8 of the Charter of Fundamental Rights and Article 16(2) TFEU, specifically with regard to law enforcement's use of real-time biometric identification in public areas. However, the Proposal does not have any clear provisions ensuring such oversight by DPAs. Only GDPR and LED supervisory agencies may engage in market surveillance, maybe

[187] ibid.
[188] n 55, 15 – 17.

shared with other entities as was already suggested in Article 63(5) of the proposal[189] (Article 74 of the final Act). According to the EDPB and EDPS, this does not satisfy the independent supervision requirements of EU primary law.[190]

Having multiple enforcement bodies thus raises concerns about regulatory fragmentation. In cases where AI-driven processing violates both the GDPR and the AI Act, it is unclear which authority holds primary enforcement power and thereby creates uncertainty for both regulators and stakeholders.

4.6. Conclusion

The enforcement landscape of the GDPR and the AI Act show that they both have shared foundations and structural divergences that pose significant challenges for coherent regulatory oversight in the EU. While both frameworks have a predominantly decentralized enforcement model, the GDPR's experience underscores the risks of fragmentation, uneven application and capacity gaps which are issues that could recur under the AI Act if not addressed proactively. The introduction of bodies on the EU level such as the AI Office and the European AI Board could potentially make for better coordination yet these mechanisms are still limited in scope and authority especially concerning high-risk AI applications.

The overlap in supervision between national DPAs and the new authorities established under the AI Act further adds to the regulatory complexity. Without any clear allocation of responsibilities or binding cooperation mechanisms, jurisdictional conflicts and legal uncertainty are likely especially in cases where AI systems process personal data. With its proposition on the designation of DPAs as supervisory authorities for AI systems involving personal data, the joint Opinion of the EDPB and the EDPS rightly emphasizes the need for stronger integration of data protection oversight into the AI Act's governance framework.

Ultimately, effective enforcement of both the GDPR and the AI Act will depend on institutional coordination and adequate resourcing as well as on the political will to ensure independence, consistency and legal clarity. As AI technologies become increasingly intertwined with data processing, the EU has to confront the structural overlaps in its regulatory architecture to uphold fundamental rights and foster legal certainty for developers, deployers and individuals alike.

[189] n 3.
[190] n 185, 14 and 15.

This chapter has shown that despite their shared objectives, the GDPR and the AI Act diverge in some ways that can pose legal, institutional and practical challenges. These include the lack of a clearly defined legal basis for AI-driven data processing, tensions around explainability and human oversight as well as overlapping enforcement structures that risk regulatory fragmentation. While both frameworks want to navigate AI in a way that respects fundamental rights, they have differences in scope, timing and logic of intervention which complicate efforts at seamless integration. These findings show the need for clearer interpretive guidance, more robust institutional cooperation and a more future-oriented regulatory strategy. The next chapter builds on this to explore broader policy implications and consider how the EU can ensure a trustworthy and rights-based approach to AI governance in practice.

5. Policy Implications and Future Outlook

The evolving regulatory landscape of the EU shaped by the GDPR and the AI Act shows a broader ambition to safeguard fundamental rights in an era of rapid technological advancement. While both are rooted in human dignity, transparency and accountability, their parallel application raises several implications and questions and highlights the need for future regulatory evolution.

A key challenge lies in guaranteeing regulatory coherence and harmonization. AI developers and deployers must follow a dual compliance regime. While the AI Act imposes system-level obligations with a focus on risk management and technical standards, the GDPR the continues to regulate personal data processing through individual rights and legal bases. This intersection often leads to uncertainties especially regarding consent, legal justifications for large-scale data use and the enforceability of rights like explainability and human oversight. In this context, enhanced cooperation between supervisory authorities is essential. The European Data Protection Board and the newly established European Artificial Intelligence Board are going to need to collaborate closely to provide a unified and clear path to avoid fragmented enforcement.

Moreover, the dynamic nature of AI systems through machine learning, continual adaptation and sometimes opaque algorithmic decision-making, poses difficulties for traditional legal approaches grounded in predictability and linear data flows. While the GDPR has proven strong and adaptable, the raise of AI calls for continuous regulatory reflection. Delegated acts under the AI Act or interpretive guidance from the European Commission and

supervisory authorities may serve as necessary tools to keep up with the technological developments in AI.

Another pressing issue is the institutional capacities and governance models which are needed to oversee AI effectively. Data Protection Authorities have already taken on significant roles in scrutinizing AI applications under the GDPR especially in areas like biometric surveillance and profiling. As the AI Act entered into force, there now is growing recognition that DPAs, given their expertise in fundamental rights, should play a central role in AI governance when personal data is involved. This may need an expansion of their mandates, resource and technical expertise to ensure effective oversight in a rapidly this evolving digital environment.

From the perspective of stakeholders and innovators, legal certainty and regulatory clarity are the most important aspect. The parallel application of the GDPR and AI Act has to be navigable, predictable and proportionate. Clear guidance on permissible data reuse, valid forms of consent in AI contexts as well as practical implementation of obligations like transparency and human oversight will be critical to ensure that regulatory complexity does not slow down innovation or disincentivize the adoption of trustworthy AI solutions.

Looking at the future, the convergence of the GDPR and the AI Act signals a potential move towards a holistic digital rights framework in the EU being one that not only addresses privacy and data protection but also incorporates ethical governance, algorithmic accountability and democratic control over digital technologies. Regulatory instruments such as the Digital Services Act and the Data Governance Act should build upon this foundation to create an integrated, interoperable system that places fundamental rights at the heart of Europe's digital transformation.

In conclusion, the alignment of the GDPR and AI Act has opportunities as well as challenges. Their joint application already provides a powerful mechanism to ensure that AI systems in the EU are developed and used in a way that respects individual rights as well as societal values. However, achieving this vision will require not only legal precision but also institutional coordination and forward-looking policy strategies. A dynamic, principle-based and risk-sensitive regulatory approach will be essential for fostering public trust and ensuring that technological progress serves the broader public good.

6. Final Words

This thesis has thoroughly analysed the evolving relationship between the two fundamental instruments of European digital regulation, the AI Act and the GDPR. The interaction in

safeguarding fundamental rights particularly concerning privacy and personal data within the context of AI-driven technologies was analysed. While the GDPR has become a global benchmark for data protection, the AI Act now introduced a risk-based regulatory model for AI systems especially those considered high-risk. As AI increasingly relies on personal data, the intersection between these regimes becomes more significant by offering both opportunities for mutual reinforcement and also posing new legal and practical challenges. Common regulatory principles such as transparency, accountability, fairness and human oversight arise from both frameworks though via different mechanisms. The GDPR prioritizes ex post individual rights and autonomy whereas the AI Act emphasizes ex ante systemic controls and market-driven compliance.

This thesis has identified clear points of alignment including the use of Data Protection Impact Assessments (DPIAs) and Fundamental Rights Impact Assessments (FRIAs), risk-based classification and robust data governance measures. However, there still are some uncertainties especially around enforcement, legal foundations for data processing and the transparency of complex algorithmic decisions. These difficulties highlight the need for more legal clarity, institutional collaboration and maybe further specific legislative guidance.

The overarching conclusion is that regulatory consistency in this case is not just technological undertaking but also political and normative. Effectively aligning the GDPR and the AI Act needs more than mere procedural harmonisation as it also demands a collective European vision of digital governance that preserves democratic principles and the rule of law. Innovation should be promoted, provided it does not impact individual rights and liberties negatively.

In the long term, this regulatory space will continue to evolve through judicial interpretation, technological advancement and societal input. This thesis advances the discourse by demonstrating existing legal conflicts and suggesting methods for a more cohesive framework. The relationship between the GDPR and the AI Act will ultimately test the EU's ability to advise on technological innovation while safeguarding human dignity, autonomy and most importantly fundamental rights. Connecting these two legal frameworks is not simply an issue of administrative consistency, it also constitutes a normative effort that will shape the parameters of European digital sovereignty in the 21st century.

Bibliography

Table of cases

CJEU

Deutsche Telekom AG v Bundesrepublik Deutschland (Case C-543/09) [2011] ECR 2011 I-03441

GC and Others v Commission nationale de l'informatique et des libertés (CNIL) (C-136/17) [2019] ECLI:EU:C:2019:773

Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (C-507/17) [2019] ECLI:EU:C:2019:772

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) [2014] ECLI:EU:C:2014:317

Huber v Germany (C-524/06) [2008] ECLI:EU:C:2008:724

Meta Platforms Inc and Others v Bundeskartellamt (C-252/21) [2023] CLI:EU:C:2023:537

Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (C-61/19) [2020] ECLI:EU:C:2020:901

OQ v Land Hessen (C-634/21) [2023] ECLI:EU:C:2023:957

Patrick Breyer v Bundesrepublik Deutschland (C-582/14) [2016] ECLI:EU:C:2016:779

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen (C-92/09 and C-93/09) [2010] ECR 2010 I-1106

Other jurisdictions

Kennzeichenerfassung (2008) BVerfG 1 BvR 2074/05, 1 BvR 1254/07

Legislation

Charter of the Fundamental Rights of the European Union [2012] OJ C 326/393

Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/1

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS 108

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 [1995] OJ L281/31

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L1689

Secondary Sources

Books

Manoj M, Remya M and Nitha T M, *The New Intelligence: Exploring the AI Revolution* (Xoffencer international book publication house 2025)

Wittershagen L, *'The Transfer of Personal Data from the European Union to the United Kingdom Post-Brexit'* (De Gruyter 2023) <https://doi.org/10.1515/9783110988253> accessed 20 March 2025

Articles

Ajoodha T and Browne J, 'Fundamental Rights Impact Assessments:
Artificial Intelligence and automated individual decision making, including profiling, under Art. 22 GDPR' (*fieldfisher*, 30 June 2023)
<https://www.fieldfisher.com/en/insights/artificial-intelligence-and-automated-individual-decision-making> accessed 10 April 2025

Benneh Mensah G, ‘Artificial Intelligence and Ethics: A Comprehensive Review of Bias Mitigation, Transparency, and Accountability in AI Systems’ (2023) <DOI:10.13140/RG.2.2.23381.19685/1> accessed 15 April 2025

Cancela-Outeda C, ‘The EU's AI act: A framework for collaborative governance’ (2024) 27(3) Internet of Things 101291 <https://doi.org/10.1016/j.iot.2024.101291> accessed 22 March 2025

De Streel A, Bibal A, Frenay B and Lognoul M, ‘Explaining the Black Box: when law controls AI’ (*cerre Centre on Regulation Europe*, 3 February 2020) <https://cerre.eu/wp-content/uploads/2020/03/issue_paper_explaining_the_black_box_when_law_controls_ai.pdf> accessed 21 April 2025

D'hulst T and Kloza D, ‘Data protection impact assessment: More than just a compliance tool’ (*Van Bael & Bellis,* 25 November 2022) <https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf> accessed 28 March 2025

Díaz-Rodríguez N, Javier Del Ser, Mark Coeckelbergh and others, ‘Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation’ (2023) 99 Information Fusion 101896 <https://doi.org/10.1016/j.inffus.2023.101896> accessed 23 April 2025

Gryz J and Rojszczak M, ‘Black box algorithms and the rights of individuals: no easy solution to the “explainability” problem’ (2021) 10(2) Internet Policy Review <https://doi.org/10.14763/2021.2.1564> accessed 25 April 2025
Hacker P, ‘Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law’ (2018) 55(4) Common Market Law Review <https://ssrn.com/abstract=3164973> accessed 20 April 2025

Hacker P, Cordes J and Rochon J, ‘Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond’ (2023) 15(1) European Journal of Risk Regulation 49 <https://doi.org/10.1017/err.2023.81> accessed 25 April 2025

Hoofnagle CJ, van der Sloot B and Zuiderveen Borgesius F, 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 65 <https://doi.org/10.1080/13600834.2019.1573501> accessed 21 April 2025

Hupont I, Micheli M, Delipetrev B, Gómez E and Soler Garrido J, 'Documenting High-Risk AI: A European Regulatory Perspective' (2023) 56(5) Computer 18 <https://dx.doi.org/10.1109/MC.2023.3235712> accessed 25 March 2025

Khalid N, Qayyum A, Bilal M and others, 'Privacy-preserving artificial intelligence in healthcare: Techniques and applications' (2023) 158 Computers in Biology and Medicine 106848 <https://doi.org/10.1016/j.compbiomed.2023.106848> accessed 20 April 2025
Kosznik-Biernacka S, 'The Analysis of Risks to Personal Data Security' (2020) 34(34) Security Dimensions 256 < DOI 10.5604/01.3001.0014.5614> accessed 10 April 2025

Lazcoz G and de Hert P, 'Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities' (2023) 50 Computer Law & Security Review 105833 <https://doi.org/10.1016/j.clsr.2023.105833> accessed 12 April 2025

Levitina A, 'Humans in automated decision-making under the GDPR and AI Act' in Colomina Saló C, Innerarity D and Cantero Gamito M (eds.), *Algorithmic inequality: governance, representation and rights in AI* (CIDOB 2024) <https://www.cidob.org/sites/default/files/2025-02/121-143_ANNA%20LEVITINA_ANG.pdf> accessed 19 April 2025

Mantelero A, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024) 54 Computer Law & Security Review 106020 <https://doi.org/10.1016/j.clsr.2024.106020> accessed 24 March 2025

Metikoš L and Ausloos J, ‘The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act’ (2025) 17(1) Law, Innovation and Technology 8 <https://doi.org/10.1080/17579961.2025.2469349> accessed 11 April 2025

Miao M, ‘Debating the Right to Explanation: An Autonomy-Based Analytical Framework’ (2022) 34 Singapore Academy of Law Journal 864 <https://dx.doi.org/10.2139/ssrn.4225103> accessed 25 April 2025

Oladipupo Amoo O, Atadoga A, Osasona F, Oluwaseun Abrahams T, Ayinla BS, Farayola O and Amoo K, ‘GDPR's impact on cybersecurity: A review focusing on USA and European practices’ (2024) 11(1) International Journal of Science and Research Archive <10.30574/ijsra.2024.11.1.0220> accessed 20 April 2025

Rudin C and Radin J, ‘Why Are We Using Black Box Models in AI When We Don’t Need To? A Lesson From an Explainable AI Competition’ (2019) 1(2) Harvard Data Science Review <https://doi.org/10.1162/99608f92.5a8a3a3d> accessed 10 April 2025

Söderlund K and Larsson S, ‘Enforcement Design Patterns in EU Law: An Analysis of the AI Act’ (2024) 3 Digital Society <https://link.springer.com/content/pdf/10.1007/s44206-024-00129-8.pdf> accessed 26 April 2025

Thelisson E and Verma H, ‘Conformity assessment under the EU AI act general approach’ (2024) 4 AI Ethics <https://doi.org/10.1007/s43681-023-00402-5> accessed 14 April 2025

Truby J, Brown RD, Ibrahim IA and Caudevilla Parellada O, ‘A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications’ (2021) 13 European Journal of Risk Regulation 270 <https://ssrn.com/abstract=4373418> accessed 23 March 2025

van Bekkum M, ‘Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI act’ (2025) 56 Computer Law & Security Review 106115 <https://doi.org/10.1016/j.clsr.2025.106115> accessed 12 April 2025

— — and Zuiderveen Borgesius F, ‘Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?’(2023) 48 Computer

Law & Security Review 105770, <https://doi.org/10.1016/j.clsr.2022.105770> accessed 12 April 2025

von Grafenstein M, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR' (2020) 6(4) EDPL 509 <https://doi.org/10.21552/edpl/2020/4/7> accessed 22 March 2025

Other secondary sources

Bettelhäuser PF, 'AI & the Right to be Forgotten under the GDPR' (Master Thesis, Lund University 2022) <http://lup.lub.lu.se/student-papers/record/9082521> accessed 11 April 2025

Clark J, Demircan M and Kettas K, 'Europe: The EU AI Act's relationship with data protection law: key takeaways' (*DLA PIPER*, 25 April 2024) <https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/> accessed 31 March 2025

Commission, 'Communication: Building Trust in Human Centric Artificial Intelligence' COM(2019) 168 final

Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final

Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final

De Luca S and Federico M, 'Algorithmic discrimination under the AI Act and the GDPR', (At a Glance, EPRS | European Parliamentary Research Service, 26 February 2025) <https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATA(2025)769509_EN.pdf> accessed 19 April 2025

Gasimova C, ‘Privacy and Transparency in an AI-driven World: Does Algorithmic Transparency Fit on Data Privacy Under GDPR?’ (Master Thesis, Lund University 2023) <http://lup.lub.lu.se/student-papers/record/9119730> accessed 26 April 2025

Hajduk P, ‘AI Act and GDPR: On the path towards overlap of the enforcement structures’ (*RAILS Robotics and AI Law Society*, 1 October 2023) <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/> accessed 30 April 2025

Hamon R, Junklewitz H and Sanchez I, ‘Robustness and Explainability of Artificial Intelligence’ (*Publications Office of the European Union,* 2020) 10 <doi:10.2760/57493> accessed 15 April 2025

Jackson S and Berger JM, ‘The Dangers of Generative AI and Extremism’ (*Middlebury Institute of International Studies*, 12 December 2023) <https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/dangers-generative-ai-and-extremism> accessed 20 April 2025

Kopp N, ‘Legal bases for data processing by AI’ (*activeMind.legal*, 30 September 2024) <https://www.activemind.legal/guides/legal-bases-ai/> accessed 15 April 2025

Madiega T, ‘Artificial intelligence act’ [2024] European Parliamentary Research Service <https://www.dirittobancario.it/wp-content/uploads/2024/09/Documento-riassuntivo-dellAI-Act-Parlamento-europeo-settembre-2024.pdf> accessed 10 April 2025

Nannini L, ‘Habemus a Right to an Explanation: so What? – A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act’ (2024) 7(1) Proceedings of the Seventh AAAI/ACM Conference on AI, Ethics, and Society (AIES-24) <https://doi.org/10.1609/aies.v7i1.31700> accessed 10 April 2025

Panigutti C, Hamon R, Isabelle Hupont and others, ‘The role of explainable AI in the context of the AI Act’ (Conference: FAccT '23: the 2023 ACM Conference on Fairness, Accountability, and Transparency, June 2023) <https://dl.acm.org/doi/pdf/10.1145/3593013.3594069> accessed 10 April 2025

Punie M, ‘The GDPR and the AI Act: A Harmonized Yet Complex Regulatory Landscape’ (*datenschutznotizen*, 22 January 2025) <https://www.datenschutz-notizen.de/the-gdpr-and-the-ai-act-a-harmonized-yet-complex-regulatory-landscape-1151788/> accessed 24 March 2025

Westlund M, ‘The development of the right to privacy under the ECHR’ (Master’s Thesis in Public International Law, Uppsala Universitet 2018) <http://www.diva-portal.org/smash/get/diva2:1257161/FULLTEXT01.pdf> accessed 20 March 2025

Žunić Marić T, Đukanović J and Spasojević D, ‘Comparing the obligations under the GDPR and AI Act - where is the overlap?’ (*lexology*, 22 October 2024) <https://www.lexology.com/library/detail.aspx?g=5487aa15-1408-4564-bcfe-7138a3869268#> accessed 23 March 2025

‘Accountability’ (*European Data Protection Supervisor*) <https://www.edps.europa.eu/data-protection/our-work/subjects/accountability_en> accessed 1 April 2025

‘AI Act’ (*European Commission*, 18 February 2025) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 15 March 2025

‘AI Board’ (*European Commission*, 24 March 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-board> accessed 24 March 2025

‘Artificial intelligence: stop to ChatGPT by the Italian SA
Personal data is collected unlawfully, no age verification system is in place for children’ (*GPDP Garante per la protezion dei dati personali*, 20 December 2024) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847> accessed 30 April 2025

‘Data Minimization as a Tool for AI Accountability’ (*AI Now Institute*, 11 April 2023) <https://ainowinstitute.org/publications/data-minimization> accessed 30 March 2025

‘Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition’ (*Autoriteit Persoonsgegevens*, 3 September 2024) <https://autoriteitpersoonsgegevens.nl/en/current/dutch- dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition> accessed 12 April 2025

‘Ethics Guidelines for trustworthy AI’ (*European Commission*, 8 April 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> accessed 15 April 2025

‘General Purpose AI and the AI Act’ (*future of life Institute*, May 2022) 3 <https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf> accessed 21 April 2025

‘Governance and enforcement of the AI Act’ (*European Commission*, 17 February 2025) <https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement> accessed 15 March 2025

Guidelines 05/2020 on consent under Regulation 2016/679 adopted on 4 May 2020 [2020] <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf f> accessed 28 April 2025

Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects [2019] <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 28 April 2025

‘What is a DPIA?’ (*ico. Information Commissioner’s Office*) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/> accessed 31 March 2025

‘Handbook on European data protection law’ (*Publications Office of the European Union,* 2018) <doi:10.2811/343461> accessed 25 April 2025

Joint Opinion 5/2021 of 18 June 2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence

(Artificial Intelligence Act) [2021] <https://www.edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 31 March 2025

Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework of 16 July 2024 [2024] <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> accessed 3 April 2025