WHITE PAPER

Understanding the interaction between the EU AI Act and the GDPR

DPO Consultancy
Experts in Data Privacy

NOVEMBER 2024

Aditya Tannu
Emine Bilsin

I. Introduction

The European Union's Artificial Intelligence Act (AI Act)[1] and the General Data Protection Regulation (GDPR)[2] represent two pivotal pieces of legislation in the EU's digital regulatory framework. The AI Act, which entered into force on August 1, 2024, aims to foster responsible artificial intelligence development and deployment in the European Union (EU). It addresses potential risks to health, safety, and fundamental rights of natural persons, while providing clear requirements and obligations for AI developers and deployers (read as users). This groundbreaking legislation is the world's first comprehensive attempt to regulate AI systems and models, reflecting the EU's commitment to ethical and trustworthy AI.

The GDPR on the other hand has been in effect since May 25, 2018, and sets out rules for the protection of personal data and the free movement of such data within the EU. As AI systems may often process substantial amounts of personal data, understanding the interaction between these two regulations is paramount for organizations developing or deploying AI systems in the EU.

The interplay between the AI Act and the GDPR is complex and multifaceted. While both regulations share common goals of protecting individuals' rights and ensuring responsible use of technology, they approach these objectives from different angles. The AI Act focuses on the specific risks posed by AI systems, while the GDPR addresses the broader issues of personal data protection.

This White Paper explores the key provisions of the AI Act and it's overlapping areas with the GDPR, and the practical implications for businesses operating in the EU. By examining the interplay between these regulations, we aim to provide insights into how organizations can navigate the complex landscape of AI governance and data protection in the EU.

[1] Regulation (Eu) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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 L, 2024/1689 **("AIA")**

[2] 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 L 119/1 **("GDPR")**

II. The EU AI Act: A Detailed Overview

a. Objectives and Scope

The EU AI Act introduces a uniform framework across all EU countries, based on a forward-looking definition of AI and a risk-based approach. The primary objectives of the AI Act are to:

- Ensure that AI systems placed on the EU market and used in the EU are safe and respect existing law on fundamental rights and Union values[3].
- Ensure legal certainty to facilitate investment and innovation in AI.
- Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems.
- Facilitate the development of a single market for lawful, safe, and trustworthy AI applications and prevent market fragmentation.

The Act deals with AI systems and AI models. **AI systems** are defined as machine-based systems that function with some autonomy, have a given set of implicit or explicit objectives and generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with due to an intrinsic ability to infer how to generate such output. As such, AI systems can be said to have three main components: perception (of input data), reasoning/decision making (processing) and actuation (through output). **AI models** on the

[3] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012

other hand are computational structures or algorithms that are trained on certain datasets to generate output when provided with certain input data. Therefore, they form the processing component of an AI system. AI models lack certain components needed to be classified as AI systems. For instance, ChatGPT (an AI system) provides users with an interface (such as the chat window) to interact with it. It is built on several different AI models such as GPT-3.5, GPT-4o, and so on.

The Act's risk-based approach operates by designating four risk levels.

1. **Unacceptable risk:** Article 5 refers to these as 'prohibited practices'. AI systems that pose a clear threat to people's safety, livelihoods, and rights are banned. These include social scoring systems by governments, AI-enabled manipulation of human behavior and real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes (with some exceptions). AI systems with this risk level are to be put out of service by 2nd February 2025.

2. **High risk:** AI systems that could harm people's safety or fundamental rights must comply with strict requirements. This category includes AI systems used in critical infrastructure (such as transport and supply of electricity), educational or vocational training and several other use-cases listed under Annex III of the Act.

3. **Limited risk:** Article 50 refers to these as 'AI systems with certain risks' that arise when using generative and interactive AI systems. These include chatbots, emotion recognition systems, biometric categorization systems and AI systems that generate or manipulate image, audio, or video content (deepfakes).

4. **Systemic risk:** Unlike the above risks, systemic risks can only be found in General-Purpose AI Models (GPAIMs). These are AI models trained on large amounts of data, which display generality in their use and have high impact capabilities (cumulative amount of computation used for training, when measured in floating point operations, is greater than 10^{25}).

b. Roles and Responsibilities

The AI Act defines several key roles and their associated responsibilities. The most prominent are as follows:

1. **Providers[4]:** These include organizations that develop an AI system and place it on the market or put it into service. The definition covers extra-territorial entities as well. For instance, a multinational tech company based in the US develops an AI system for medical diagnosis. They plan to market this system in the EU under their brand.

[4] Art. 3(3), AIA.

Despite being based outside the EU, they are considered a provider under the AIA for their EU operations as making their AI system available in the EU qualifies as placing it on the market. Providers undertake the major burden of regulatory compliance, and their responsibilities include:

- Ensuring that high-risk AI systems comply with the requirements set out in the Act.
- Implementing a quality management system
- Drawing up technical documentation
- Conducting Conformity Assessments
- Registering high-risk AI systems in the EU database
- Taking corrective actions when necessary
- Cooperating with national competent authorities

2. **Deployers[5]:** These refer to natural or legal persons using an AI system under their authority, except where the AI system is used during a personal non-professional activity. Typically, these can be referred to as the 'users' of an AI system. Currently, most organizations do not develop their own AI system and therefore a large chunk of organizations could classify as deployers of AI systems. It is important to note that even if an AI system is not developed by an entity, if such an entity attaches their trademark to a procured AI system, they are classified as a provider under the AIA. Some of deployers responsibilities include:
   - Using high-risk AI systems in accordance with the instructions of use
   - Ensuring human oversight when using high-risk AI systems.
   - Conducting Fundamental Rights Impact Assessments where appropriate.
   - Monitoring the operation of high-risk AI systems based on the instructions of use.
   - Informing the provider or distributor about any serious incident or malfunctioning.

3. **Importers[6]:** Any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union. Some of their responsibilities include:
   - Ensuring that the appropriate Conformity Assessment procedure has been conducted by the provider.
   - Ensuring that the technical documentation is available.
   - Ensuring that the AI system bears the required conformity marking and is accompanied by the required documentation and instructions of use.

[5] Art. 3(4), AIA.
[6] Art. 3(6), AIA.
[7] Art. 3(7), AIA.

4. **Distributors[7]:** Any natural or legal person in the supply chain, other than the provider or the importer, which makes an AI system available on the Union market without affecting its properties. Their responsibilities include:
   - Verifying that the AI system bears the required conformity marking and is accompanied by the required documentation.
   - Ensuring that storage or transport conditions do not jeopardize the AI system's compliance.

Compliance obligations vary depending on **the risk level of the AI system** and **the role of the organization in the AI supply chain**. For high-risk AI systems, providers must conduct Conformity Assessments, implement risk management systems, and ensure human oversight.

c. Enforcement and Penalties

The AI Act establishes a robust enforcement mechanism to ensure compliance:

1. **National Market Surveillance Authorities:** Authorities under the EU Regulation 2019/1020 on market surveillance and compliance of products[8] will lead the way in undertaking compliance investigations and enforcement actions under the AI Act.

2. **European Artificial Intelligence Board and Office:** The AI Board is a new legal entity established by the Act. It is tasked with advising and assisting the Commission and Member States in facilitating the consistent and effective application of the Act. The AI office on the other hand is a Commission function that has monitoring and supervising tasks to develop expertise and capabilities of the EU market in the field of AI.

3. **Penalties:** The AI Act sets out significant penalties for non-compliance, which can be applied starting 2nd August 2025[9]:
   - Up to €35 million or 7% of the company's total worldwide annual turnover for violating prohibited AI restrictions.[10]
   - Up to €15 million or 3% of turnover for certain other infringements.[11]
   - Up to €7.5 million or 1% of turnover for the supply of incorrect, incomplete, or misleading information to competent authorities.[12]

These penalties are designed to be effective, proportionate, and dissuasive, reflecting the potential impact of AI systems on fundamental rights and safety.

[7] Art. 3(7), AIA.

[8] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.6.2019, p. 1–44.

[9] Art. 113, AIA.

[10] Art. 99(3), AIA.

[11] Art. 99(4), AIA.

[12] Art. 99(5), AIA.

III. The GDPR's Relevancy for Artificial Intelligence

In the current technological landscape, most AI systems are opaque in terms of their functioning and the data used to their underlying models. Several GDPR concepts are particularly relevant here:

1. **Data Protection by Design and by Default:** Article 25 GDPR requires organizations to implement appropriate technical and organizational measures to integrate data protection into their processing activities and business practices.

2. **Data Protection Impact Assessments (DPIAs):** Article 35 GPDR mandates that where a type of processing, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

3. **Automated Individual Decision-Making:** Article 22 GDPR provides that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

4. **Transparency:** Articles 13 and 14 GDPR require that data subjects be provided with information about the processing of their personal data, including meaningful information about the logic involved in automated decision-making systems.

Due to these concepts, and the longstanding enforcement mechanism of the GDPR, there are significant implications for AI applications, particularly in areas such as:

1. **Big Data and Machine Learning:** The principles of purpose limitation and data minimization can pose challenges for AI systems that rely on large datasets and may discover new insights or purposes for data during processing.

2. **Automated Decision-Making:** The GDPR's provisions on automated decision-making and profiling require organizations to provide human intervention, express data subjects' point of view, and contest decisions made by AI systems in certain circumstances.

3. **Explainability and Transparency:** The GDPR's requirements for transparency and the right to explanation can be challenging for complex AI systems, particularly those using deep learning or neural networks.

4. **Data Protection Impact Assessments:** Organizations developing or deploying AI systems that process personal data may need to conduct DPIAs to assess and mitigate risks to data subjects.

IV. Interplay Between the EU AI Act and GDPR

a. Complementary Nature

The AI Act and the GDPR are designed to work in tandem, with the AI Act complementing and building upon the data protection framework established by the GDPR. While the GDPR focuses on the protection of personal data, the AI Act addresses the broader implications of AI systems, including their potential impact on fundamental rights, safety, and societal values.

The AI Act explicitly states that it is without prejudice to the application of the GDPR, indicating that compliance with one regulation does not exempt organizations from complying with the other. This means that organizations must consider both regulations when developing and deploying AI systems that process personal data.

Key areas of complementarity include:

1. **Risk-based approach:** Both regulations adopt a risk-based approach, requiring more stringent measures for high-risk activities or systems.

2. **Fundamental rights protection:** Both aim to protect individuals' fundamental rights, with the GDPR focusing on data protection and privacy, and the AI Act addressing a broader range of rights potentially affected by AI systems.

3. **Transparency and accountability:** Both regulations emphasize the importance of transparency in data processing and decision-making, as well as the accountability of organizations.

b. Data Subject Rights and AI

The interaction between data subject rights under the GDPR and AI systems regulated by the AI Act is complex:

1. **Automated decision-making:** Article 22 of the GDPR provides safeguards against automated decision-making, including the right to human intervention, to express one's point of view, and to contest the decision. The AI Act builds on this by requiring human oversight for high-risk AI systems and prohibiting certain AI practices that could manipulate human behavior.

2. **Transparency:** While both regulations require transparency, the AI Act introduces additional requirements for certain AI systems, such as the obligation to inform users when they are interacting with an AI system. This complements the GDPR's requirements for transparent information about data processing.

3. **Right of access:** The GDPR's right of access may be challenging to implement for complex AI systems, particularly in terms of providing meaningful information about the logic involved in automated decision-making. The AI Act's requirements for documentation and traceability of high-risk AI systems may help address this challenge.

4. **Right to rectification:** The GDPR's right to rectification may be complicated in the context of AI systems, where correcting input data may not necessarily lead to a change in the system's output. The AI Act's requirements for data governance and quality may help ensure the accuracy of data used in AI systems.

5. **Right to erasure:** Implementing the GDPR's right to erasure (right to be forgotten) can be technically challenging for AI systems, particularly those using machine learning techniques. The AI Act's requirements

for documentation and traceability may help organizations track personal data through AI systems to facilitate erasure when required.

6. **Bias and discrimination:** Both regulations aim to prevent discrimination. The GDPR prohibits the processing of special categories of personal data that could lead to discrimination, while the AI Act requires high-risk AI systems to be designed and developed to prevent discriminatory outcomes. The AI Act goes further by mandating the use of high-quality training data and the implementation of bias monitoring and correction mechanisms for high-risk AI systems.

It is to be noted that the practical enforcement of data subject rights under Chapter III GDPR in the current technological landscape is uncertain and specific guidance on the intersection of GDPR and the AI Act is awaited. Currently, AI models are trained on a vast amount and array of data, and it might not be technically possible to rectify specific (or delete) personal data. A discussion paper published by the Hamburg Commission for Data Protection and Freedom of Information (HmbBfDI) on Large Language Models (LLM)[13] states that the storage of an LLM does not constitute processing within the meaning of GDPR. It also states that LLMs lack the storage of personal data and as such claims by data subjects for access, erasure, or rectification of personal data cannot relate to the foundational AI model. However, they can certainly be claimed against the providers and deployers of an AI system. It is important to note that while a trained-LLM may lack the storage of personal data, personal data is indeed processed while training such LLM. Hence, data subject rights can also be claimed during the training stage of the LLM.

c. Overlapping Areas and Distinct Provisions

Several areas where the AI Act and GDPR intersect include:

1. **Assessments:** Both regulations require organizations to assess the risks associated with their data processing activities or AI systems. The AI Act mandates risk assessments for high-risk AI systems by requiring providers of high-risk systems to conduct Conformity Assessments and deployers to conduct Fundamental Rights Impact Assessments. On the other hand, the GDPR requires Data Protection Impact Assessments (DPIAs) for high-risk data processing activities.

2. **Transparency:** Both regulations emphasize the importance of transparency. The GDPR requires organizations to provide clear information about how personal data is processed, while the AI Act mandates specific transparency requirements for certain AI systems, such as chatbots.

[13] The Hamburg Commissioner for Data Protection and Freedom of Information, "Discussion paper: Large Language Models and Personal Data", 15th July 2024, (https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf0)

3. **Human oversight:** The AI Act requires human oversight for high-risk AI systems, which aligns with the GDPR's provisions on automated decision-making and the right to human intervention.

4. **Data governance:** Both regulations emphasize the importance of proper data management practices, with the GDPR focusing on personal data protection and the AI Act addressing the quality and appropriateness of data used to train AI systems.

5. **Record-keeping and documentation:** Both regulations require organizations to maintain detailed records of their activities, with the GDPR mandating records of processing activities and the AI Act requiring technical documentation for high-risk AI systems.

Despite these overlaps, there are also distinct provisions in each regulation:

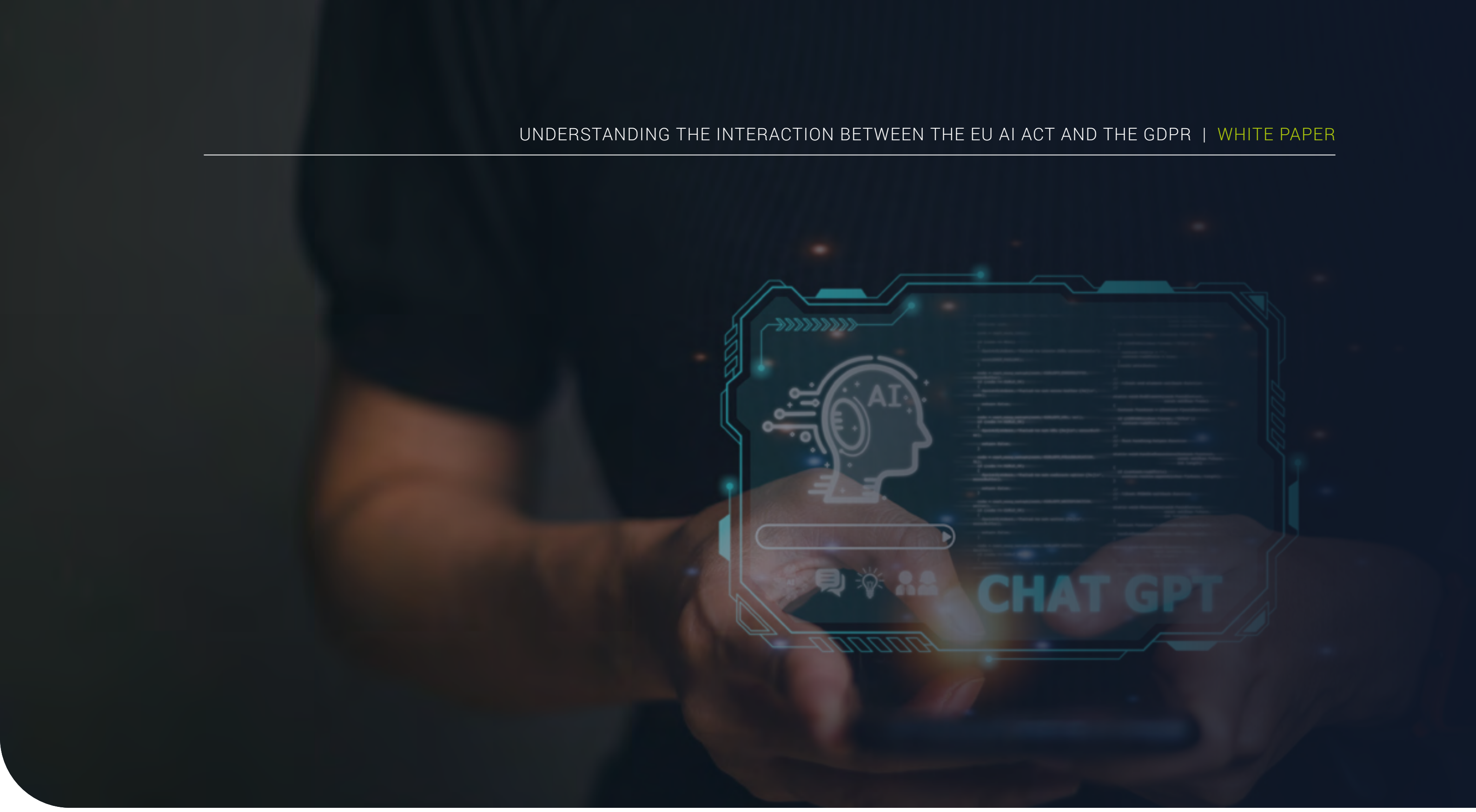
1. **Scope:** The GDPR applies to the processing of personal data, while the AI Act covers AI systems regardless of whether they process personal data.

2. **Prohibited practices:** The AI Act explicitly prohibits certain AI practices, such as social scoring by public authorities, which is not directly addressed in the GDPR. This distinction also showcases the protection of a wide range of rights under the AI Act, beyond privacy and data protection.

3. **Conformity Assessment (CA) and Fundamental Rights Impact Assessments (FRIA):** The AI Act introduces a new requirement for undertaking CAs and FRIAs of high-risk AI systems, which is not present in the GDPR.

4. **Sectoral focus:** The AI Act includes specific provisions for AI systems used sectors, such as law enforcement and border control, which are not specifically addressed in the GDPR.

A comprehensive key highlighting the approach of the EU AI Act and the GDPR to several concepts can be found in Annex I below.



V. Practical Implications for Businesses

a. Compliance Challenges and Strategies

Organizations developing or deploying AI systems in the EU must navigate compliance with both the AI Act and the GDPR. Some key challenges and strategies include:

1. **Dual compliance:** Organizations need to ensure that their AI systems comply with both the AI Act's risk-based requirements and the GDPR's data protection principles. This may require a comprehensive review of existing systems and processes.
   Strategy: Develop an integrated compliance framework that addresses both AI Act and GDPR requirements. This could involve creating cross-functional teams with expertise in AI, data protection, and legal compliance.

2. **Data governance:** Implementing robust data governance frameworks that address both AI-specific risks and data protection requirements is crucial. As the use of shadow AI (unsanctioned or ad-hoc use of AI tools) increases in organizations, it is pertinent to update the Record of Processing Activities to accurately reflect such practices, as the use of such tools can lead to data breaches. The Dutch Data Protection Authority specifically cautions against such use.[14]

[14] Autoriteit Persoonsgegevens, "Caution: use of AI chatbot may lead to data breaches", 6th August 2024, (https://www.autoriteit-persoonsgegevens.nl/en/current/caution-use-of-ai-chatbot-may-lead-to-data-breaches)

Strategy: Establish a unified data governance program that covers data quality, data minimization, purpose limitation, and data security aspects required by both regulations. This should include clear policies for data collection, use, storage, and deletion.

3. **Transparency and explainability:** Organizations must develop mechanisms to provide meaningful information about AI decision-making processes to comply with both regulations.
   Strategy: Invest in explainable AI technologies and develop clear communication protocols for informing users about AI system functionality, capabilities, and limitations. Create layered explanations suitable for different audiences (e.g., technical, legal, and general public).

4. **Human oversight:** Implementing effective human oversight mechanisms for high-risk AI systems while respecting GDPR requirements on automated decision-making.
   Strategy: Design AI systems with human-in-the-loop processes, especially for high-risk applications. Develop training programs for human overseers to ensure they understand both the technical aspects of the AI system and the relevant legal requirements.

5. **Risk assessments:** Conducting comprehensive risk assessments that satisfy both the AI Act's requirements for high-risk AI systems and the GDPR's Data Protection Impact Assessment (DPIA) obligations.
   Strategy: Develop an integrated risk assessment methodology that combines elements of both AI risk assessments and DPIAs. This could

involve creating a unified risk register that captures risks related to both AI system performance and data protection.

6. **Documentation and record-keeping:** Maintaining detailed documentation to demonstrate compliance with both regulations.
   Strategy: Implement a centralized documentation management system that captures all relevant information for both AI Act and GDPR compliance. This should include technical specifications, data flow diagrams, risk assessments, and records of data processing activities.

7. **Continuous monitoring and updating:** Ensuring ongoing compliance as AI systems evolve and regulations are updated.
   Strategy: Establish a compliance monitoring program that regularly assesses AI systems against both AI Act and GDPR requirements. Implement version control for AI models and maintain clear audit trails of system changes and compliance checks.

b. Data Protection Impact Assessments (DPIAs)

DPIAs play a crucial role in ensuring compliance with both the GDPR and the AI Act:

1. **GDPR requirement:** DPIAs are mandatory under the GDPR for high-risk data processing activities, including those involving innovative technologies like AI. Article 35 of the GDPR outlines the requirements for DPIAs, which include:
   - A systematic description of the envisaged processing operations
   - An assessment of the necessity and proportionality of the processing
   - An assessment of the risks to the rights and freedoms of data subjects
   - The measures envisaged to address the risks.

2. **AI Act integration:** Organizations can integrate AI risk assessments required by the AI Act into their DPIA processes to ensure comprehensive risk management. This integrated approach should cover:
   - Technical aspects of the AI system, including its architecture, training data, and performance metrics.
   - Potential impacts on fundamental rights, including privacy, non-discrimination, and human dignity.
   - Specific risks associated with the AI system’s intended use and deployment context.

3. **Continuous monitoring:** DPIAs should be viewed as ongoing processes, regularly updated to reflect changes in AI systems and data processing activities. This aligns with the AI Act’s requirement for continuous monitoring and updating of high-risk AI systems.

4. **Stakeholder involvement:** Both the GDPR and the AI Act emphasize the importance of involving relevant stakeholders in the risk assessment process. This may include data protection officers, AI ethics committees, and representatives of potentially affected groups.

5. **Documentation and transparency:** The outcomes of integrated DPIAs and AI risk assessments should be clearly documented and, where appropriate, made available to regulatory authorities and affected individuals.

6. **Mitigation measures:** Based on the identified risks, organizations should develop and implement appropriate mitigation measures that address both data protection and AI-specific concerns.

7. **Supervisory authority consultation:** In cases where a DPIA indicates high residual risks, organizations may need to consult with supervisory authorities, as required by the GDPR. This process may need to be coordinated with any notification requirements under the AI Act for high-risk AI systems.

By conducting comprehensive and integrated impact assessments, organizations can ensure a holistic approach to compliance that addresses the requirements of both the GDPR and the AI Act.

VI. Conclusion

The interaction between the EU AI Act and the GDPR presents both challenges and opportunities for organizations developing or deploying AI systems in the EU. While compliance with both regulations may seem daunting, their complementary nature provides a comprehensive framework for responsible AI development and deployment.

Key takeaways for organizations navigating this regulatory landscape include:

- **Integrated compliance approach:** Develop strategies that address the requirements of both regulations simultaneously, recognizing their overlaps and distinct provisions.
- **Risk-based focus:** Prioritize resources based on the risk level of AI systems and data processing activities, with particular attention to high-risk applications.
- **Privacy and ethics by design:** Incorporate data protection and ethical considerations from the earliest stages of AI system development and throughout the entire lifecycle.
- **Transparency and explainability:** Invest in technologies and processes that enhance the transparency and explainability of AI systems to meet the requirements of both regulations.
- **Human oversight:** Implement effective human oversight mechanisms, especially for high-risk AI systems and automated decision-making processes.
- **Continuous monitoring and updating:** Establish processes for ongoing compliance monitoring and regular updates to AI systems and associated documentation.
- **Stakeholder engagement:** Involve relevant stakeholders, including data protection officers, AI ethics committees, and potentially affected individuals, in the compliance process.
- **Documentation and accountability:** Maintain comprehensive documentation of compliance efforts, risk assessments, and mitigation measures to demonstrate accountability under both regulations.

By understanding the interplay between these regulations and implementing robust compliance strategies, organizations can develop and deploy AI systems that not only meet legal requirements but also foster trust and ethical use of AI technologies. As the regulatory landscape continues to evolve, staying informed and adaptable will be key to successfully navigating the intersection of AI and data protection in the EU.

The combined framework of the AI Act and the GDPR sets a global benchmark for responsible AI development and use. Organizations that successfully navigate this complex regulatory environment will be well-positioned to lead in the ethical and trustworthy AI space, potentially gaining a competitive advantage in the global market.

As AI technologies continue to advance and permeate various aspects of society, the regulatory framework will evolve as well. Organizations should remain vigilant and prepared to adapt their compliance strategies to address new challenges and requirements that may emerge at the intersection of AI governance and data protection.

Annex I: Comparison between the EU AI Act and the GDPR

Aspect	EU AI Act	GDPR
Primary Focus	Regulation of AI systems and models	Protection of personal data
Scope	AI systems, regardless of personal data processing	Processing of personal data
Risk-based Approach	Four risk levels: unacceptable, high, limited, and systemic	Risk-based approach for data processing activities
Prohibited Practices	Explicitly bans certain AI practices (e.g., social scoring)	No specific AI-related prohibitions
Assessments	Conformity Assessments (CA) and Fundamental Rights Impact Assessments (FRIA) for high-risk AI systems	Data Protection Impact Assessments (DPIA) for high-risk processing
Transparency Requirements	Specific requirements for AI systems (e.g., informing users of AI interaction)	General transparency requirements for data processing
Human Oversight	Mandatory for high-risk AI systems, not only for instances of decision-making	Right to human intervention in automated decision-making
Data Subject Rights	Indirectly addressed through system requirements	Explicitly defined (e.g., access, rectification, erasure)
Data Governance	Focus on quality and appropriateness of training data	Focus on personal data protection principles
Automated Decision-Making	Addresses through human oversight requirements	Specific provisions in Article 22
Bias and Discrimination	Explicit requirements to prevent discriminatory outcomes in AI systems	Prohibits processing of special categories of data leading to discrimination
Enforcement	National Market Surveillance Authorities, AI Board, and AI Office	Data Protection Authorities
Penalties	Up to €35 million or 7% of global turnover	Up to €20 million or 4% of global turnover
Record-keeping	Technical documentation for high-risk AI systems	Records of Processing Activities
Sectoral Focus	Specific provisions for sectors like law enforcement and not all sectors are covered by the legislation	Applicable across sectors

Europalaan 28b
5232 BC 's-Hertogenbosch
The Netherlands

Congresstraat 35
1000 Brussels
Belgium

Office 5, Rec 2, Enterprise Centre, Randall
Retford, Nottinghamshire
DN22 7GR
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com

DPO Consultancy
Experts in Data Privacy