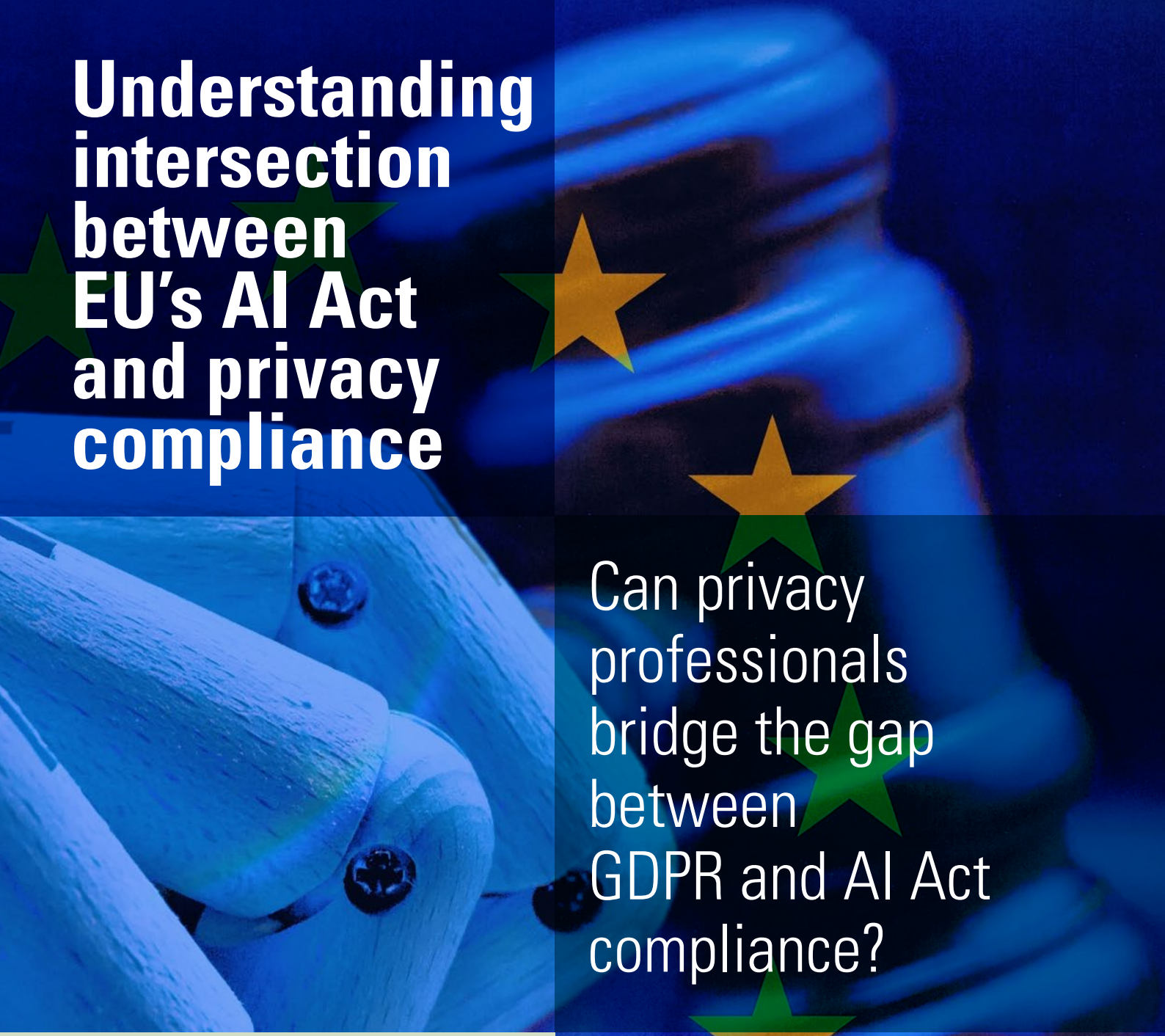
Understanding intersection between EU's AI Act and privacy compliance



Can privacy professionals bridge the gap between GDPR and AI Act compliance?

Using and implementing AI is on everyone's minds and agendas, but it can be a challenge to understand how to handle matters in a way that meets regulatory requirements and respects privacy. In this article we will unpack the EU's Artificial Intelligence Act, its journey, and its implications for privacy and compliance. We will explore the interplay between the AI Act and GDPR, and how to leverage GDPR compliance for responsible AI development and deployment.

Stephan Idema
is Director at KPMG Cyber & Privacy.

Daniela Gonzalez Riedel
is Manager at KPMG Cyber & Privacy.

INTRODUCTION

For several years, the European Union has been diligently working on the Artificial Intelligence Act (hereafter referred to as the AI Act), aimed at regulating the development and use of AI technologies. The AI Act seeks to ensure that organizations develop and utilize AI in a manner that is safe, transparent, and traceable, while also being non-discriminatory. This legislative framework builds upon the foundation laid by the EU General Data Protection Regulation (GDPR) established in 2018, which granted individuals fundamental rights concerning the protection of their personal data.

Now, the scope is expanding beyond privacy to encompass broader fundamental rights such as non-discrimination and human dignity. Although privacy remains a core element in the regulation of AI and algorithms, it is essential to recognize that most critical or "high-risk" AI systems involve the processing of (sensitive) personal data. Often, the misuse of personal data is the pivotal factor behind these emerging risks, making data privacy and protection the cornerstone for safeguarding the broader rights and freedoms of our citizens. Hence, protecting personal data and regulating AI should be viewed as interdependent rather than separate endeavors.

This article will unravel this interconnection. We will start with a brief overview of the AI Act, outlining its regulatory journey and current status. Subsequent chapters will delve into the types of AI systems, the regulatory requirements, and the connection with personal data processing under the GDPR. Following this, we will conduct a comprehensive analysis of the relationship between the AI Act and GDPR, demonstrating how GDPR compliance can be leveraged to create a responsible and compliant AI organization. The article will conclude with final remarks on the interplay between these regulatory frameworks.

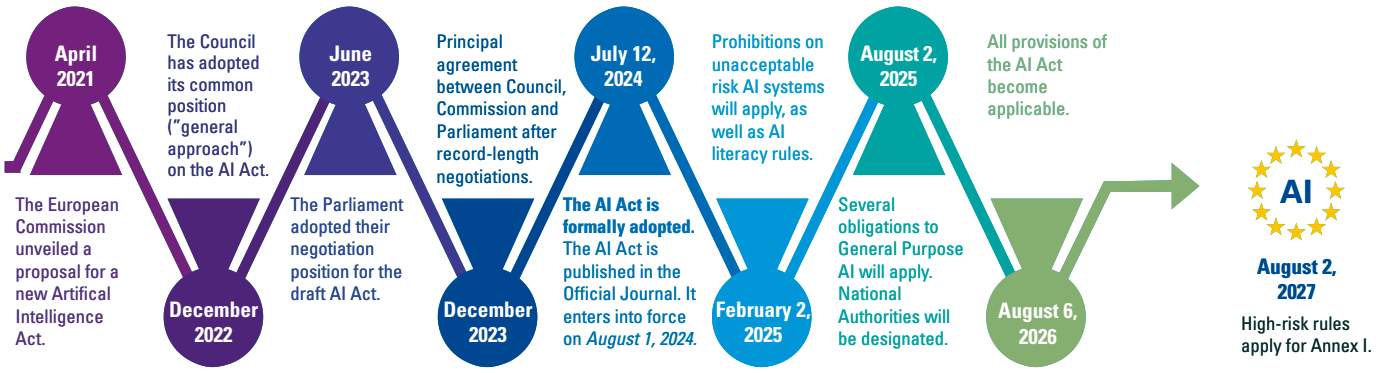


Figure 1. Legislative timeline EU AI Act.

UNDERSTANDING THE AI ACT

The Artificial Intelligence Act (AI Act) is a regulation proposed by the European Union (EU) to establish a common regulatory and legal framework for artificial intelligence (AI) within the EU. The AI Act was proposed by the European Commission on 21 April 2021 and formally adopted on 21 May 2024. It was published in the Official Journal of the European Union on 12 July of 2024, and "entered into force" on 1 August 2024.

The AI Act follows a risk-based approach and classifies AI applications into four risk categories: "unacceptable", "high", "limited", and "minimal", plus one additional category for general-purpose AI. With the entry into force of the AI Act, comes a timeline for prohibitions linked, in part, to these risk categories. Most urgently, prohibitions on unacceptable risk AI systems will take effect six months after the regulations come into force, starting on February 2, 2025.

The EU AI Act and the General Data Protection Regulation (GDPR) are both significant pieces of legislation in the European Union that regulate different aspects of technology. The GDPR is a fundamental (human) rights law that gives individuals a wide range of rights in relation to the processing of their data. On the other hand, the EU AI Act is a product safety law that provides parameters for the safe technical development and use of AI systems and is based on medical device safety legislation.

The AI Act also proposes the introduction of a European Artificial Intelligence Board to promote national cooperation and ensure compliance with the regulation. Like the European Union's General Data Protection Regulation, it can apply extraterritorially to all organizations that provide, import, distribute and/or deploy AI systems on the EU market.

The AI Act is expected to have a large impact on the economy and is considered the first comprehensive regulation on AI by a major regulator. And like the GDPR, non-compliance carries with it the potential for significant penalties. It is particularly significant following the rise in popularity of generative AI systems such as ChatGPT, Gemini, Mistral and Llama.

In summary, the EU AI Act aims to strike a balance between innovation, compliance, and responsible AI deployment, ensuring trustworthiness and respect for human rights and values. Its impact will likely extend beyond the EU, influencing global AI practices and governance.

The key roles

Under the AI Act, there are multiple roles identified within the AI value chain. The roles of providers and deployers are the key roles and play distinct yet interconnected roles within this ecosystem. Let's explore their differences and responsibilities:

Provider
Definition: A provider is a natural or legal person, public authority, agency, or other body that develops an AI system and intends to put it on the EU market.

Responsibilities:
- Develops and designs the AI system.
- Ensures compliance with AI Act requirements (Article 16).
- Provides technical documentation and instructions for use.
- Monitors and evaluates the AI system's performance.

Examples: AI software companies, research institutions, manufacturers of AI hardware.

Deployer
Definition: A deployer is any natural or legal person, public authority, agency, or other body using an AI system under its authority (except for personal non-professional activities).

Responsibilities:
- Implements the AI system within their organization or context.
- Ensures proper use and adherence to guidelines.
- May modify the AI system's intended purpose or make substantial changes.
- Communicates relevant information to end-users.

Examples: Organizations integrating AI into their operations, government agencies using AI for public services.

It is important to note that these roles are not fixed. Deployers can assume provider responsibilities under certain conditions, namely if they market the AI system under their own trademark or if they significantly modify the AI system. The distinction between providers and deployers can also blur based on system modifications and branding.

Apart from the roles of Provider and Deployer, the AI Act also identifies several other key roles within the AI value chain, which we briefly outline here. These include:
- **Product Manufacturer:** This role involves the creation of physical products that may incorporate AI systems.

- **Importer:** This role is responsible for bringing AI systems into the EU market from outside the region.
- **Distributor:** This role involves the distribution of AI systems within the market.
- **Authorized Representative:** This role represents providers or deployers who are not located in the EU but operate within the EU market.

Each of these roles carries different levels of compliance obligations, ranging from data governance and transparency to technical documentation. It is important to note that the specific obligations can vary depending on the risk level of the AI system in question. In particular, high-risk AI systems have more stringent requirements, accounting for over two thirds of requirements under the AI Act. Table 1 provides an overview of the requirements for high-risk AI systems by role ([KPMG24]).

Requirement	Provider	Importer	Distributor	Deployer
Establishment of a risk management system	✕			
Data and data governance	✕			
Technical documentation	✕	✕	✕	
Record-keeping	✕			
Transparency and provission of information to deployers	✕			
Human oversight	✕			
Accuracy, robustness and cybersecurity	✕			
Quality management system	✕			
Documentation keeping	✕			
Automatically generated logs	✕			
Conformity assessment	✕	✕		
EU declaration of conformity	✕			
Registration obligation	✕			
Information of national competent authority upon request	✕			
Affix CE marking (Article 49)		✕	✕	
Corrective actions and duty of information (Article 21)	✕			
Demonstrate conformity upon request	✕	✕	✕	
Comply with instructions for use				✕
Consider relevance & quality of input data				✕
Monitor operation of the system				✕
Execution of data protection impact assessment				✕

Table 1. AI Act obligations for high-risk AI systems per role (derived from [KPMG24]).

Risk categories and obligations

The EU AI Act takes a risk-based approach, layering obligations according to role and risk level of the AI product. The EU AI Act classifies AI systems into four risk categories, each with its own set of obligations. In addition to these risk categories, there are also requirements specific to General Purpose AI (GPAI). We will first break down the four risk categories:

Unacceptable risk: AI systems that pose a clear threat to people's safety, livelihoods, and rights fall under this category. AI applications in this category are banned. This includes AI applications that manipulate human behavior, those that use real-time remote biometric identification (including facial recognition) in public spaces, and those used for social scoring.

High-risk: High-risk AI systems have the potential to cause significant harm and are therefore regulated. The majority of obligations under the AI Act are placed on the providers (developers) of these systems. However, users (deployers) of high-risk AI systems also have certain responsibilities, albeit fewer than those of the providers. Some examples of high-risk AI systems include AI in employment, where AI is used for hiring or performance reviews, or AI systems used in critical infrastructure. The majority of requirements outlined under the AI Act, apply to AI systems in this risk level.

Limited risk: AI systems in this category are subject to lighter transparency obligations. Developers and deployers must ensure that end-users are aware that they are interacting with AI. Examples include chatbots and systems that generate or manipulate content, such as video, audio etc.

Minimal risk: This category includes the majority of AI applications currently available on the EU single market, such as AI-enabled video games and spam filters. These systems are unregulated.

The AI Act aims to provide AI developers and deployers with clear requirements and obligations regarding specific uses of AI. In this article, we won't delve deeply into these obligations. However, below is a breakdown of the key responsibilities for both deployers and providers of high-risk AI systems (see Figures 2 and 3).

General-purpose AI

The AI Act also mandates transparency requirements for General-Purpose AI (GPAI) systems. Providers must adhere to EU copyright laws and provide clear summaries of training datasets to ensure the ethical use of data.

In addition, all GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training. Free and open license GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk. All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections.

In summary, the vast majority of the AI Act and its requirements are attached to those AI systems which are considered to be high-risk. The other categories have minimal requirements, either because the system is prohibited all together, or only limitedly regulated. For this reason, it is important for an organization to understand and identify any AI systems within this category, and work towards compliance with the associated obligations.

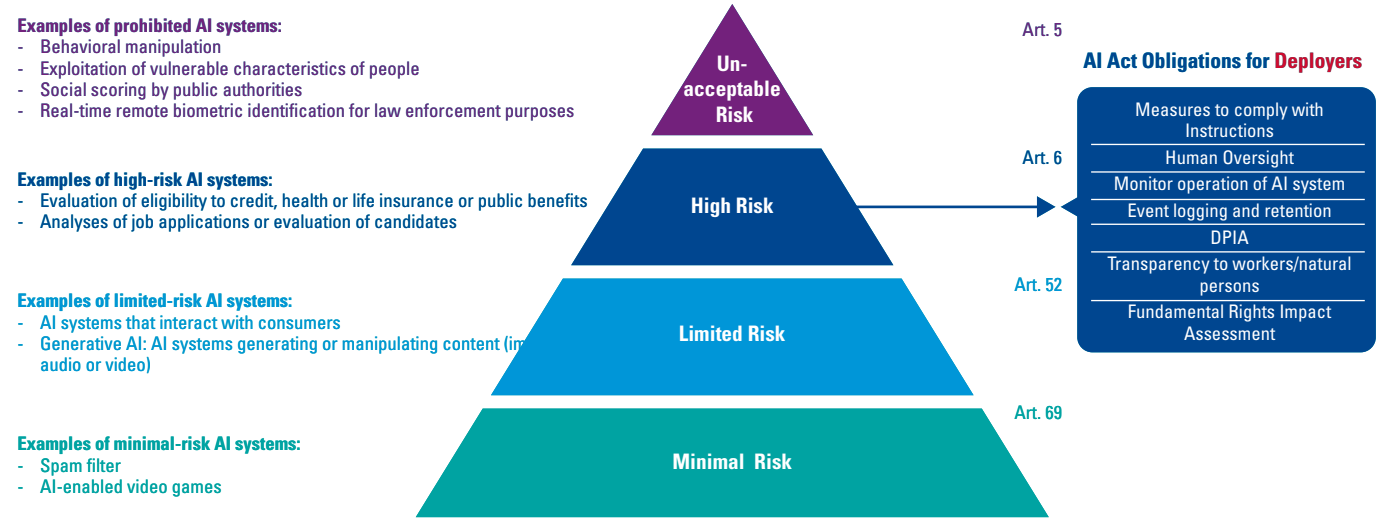


Figure 2. EU AI Act obligations for deployers of high-risk AI systems.

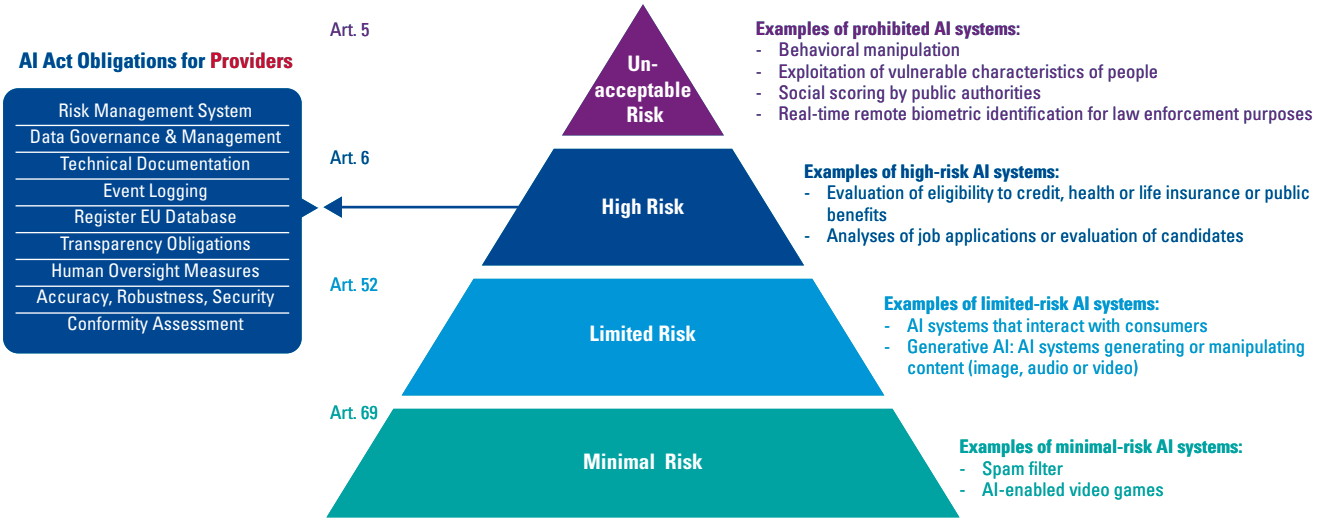


Figure 3. EU AI Act obligations for providers of high-risk AI systems.

Regulation	Maximum fine
EU AI Act	Fines up to €35 million or 7% of the company's total worldwide annual turnover, whichever is higher.
GDPR	Up to €20 million or 4% of global annual turnover, whichever is higher.
DSA (Digital Services Act)	Up to 6% of global annual turnover.
DMA (Digital Markets Act)	Up to 10% of global annual turnover, rising up to 20% of global annual turnover for repeated infringements.

Table 2. Comparison of fines per recent EU Regulation.

Consequences of non-compliance

Much like the GDPR, consequences of non-compliance with the EU AI Act can lead to significant penalties. The consequences of non-compliance with the EU AI Act will depend on the severity of the violation and the specific provisions that were breached. Consequences for non-compliance can be financial or involve (partial) ceasing of the activity/system in question. The fines are structured in a tiered system, with more severe violations carrying heftier penalties, going as high as 35 million euros or 7% of annual global turnover for violations related to AI systems that the AI Act prohibits. For comparison, Table 2 highlights that these fines are even higher than those associated with the GPDR (up to 20 million), or the Digital Services Act (up to 6% of global turnover).

Overall, the consequences of non-compliance with the EU AI Act are significant, both in terms of financial penalties, operations and reputational damage. Therefore, organizations operating within the EU or targeting EU markets should take proactive steps to ensure compliance with the requirements of the legislation. In the next section, we will explore some of these compliance enhancing measures from a privacy perspective.

PRIVACY AND THE AI ACT

Introduction and overview

The GDPR applies to AI systems to the extent that personal data is present somewhere in the lifecycle of an AI system. It is often technically very difficult to separate personal data from non-personal data, which increases the likelihood that AI systems process personal data at some point within their lifecycle. In addition, much of the data that forms the basis of AI systems, including large language models (LLMs), contains personal data.

Organizations will need to map their data very carefully to identify which elements are subject to the AI Act or the GDPR requirements, or both.

High-risk AI systems

The AI Act outlines eight typologies of high-risk AI systems, with 7 of these 8 involving a high degree of (sensitive) personal data processing. This means that in almost 90% of cases involving a high-risk AI system, compliance with GDPR is also likely necessary. Therefore, a coordinated approach to managing high-risk systems is crucial to ensure obligations are met for both the AI Act and GDPR.

The eight high-risk typologies are:

1. Biometric Identification and Categorization
2. Critical Infrastructure Management
3. Educational and Vocational Training
4. Employment, Workers Management, and Access to Self-employment
5. Essential Private and Public Services
6. Law Enforcement
7. Migration, Asylum, and Border Control Management
8. Administration of Justice and Democratic Processes

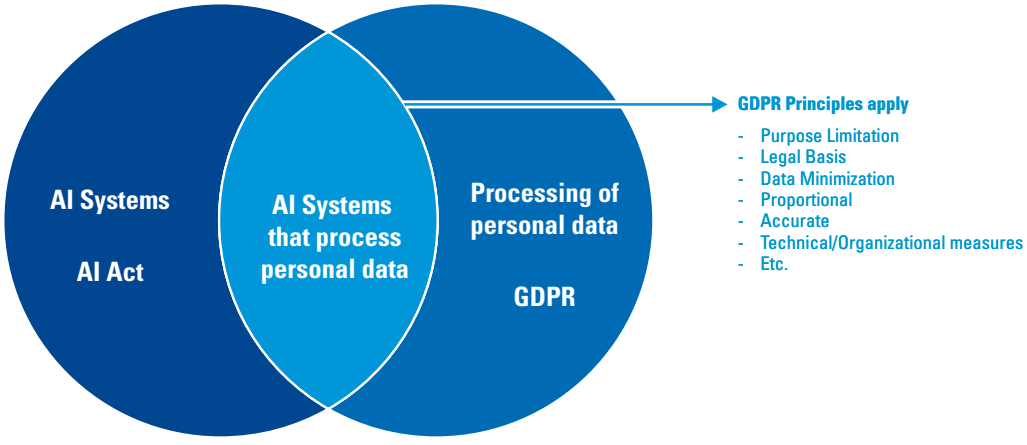


Figure 4. Intersection between AI and Privacy regulation – overlapping priorities.

For a detailed breakdown of the privacy intersections with these typology of high-risk AI systems, please refer to the appendix.

Not only do these high-risk AI systems involve personal data, they also generally involve the processing of special categories of personal data (also known as sensitive personal data), and/or involve high-risk processing activities, as defined in the GDPR. Under the GDPR, the processing of these special categories of personal data is subject to stricter requirements and additional safeguards to protect individuals' fundamental rights and freedoms. In most cases, processing such data is prohibited unless specific conditions apply, such as explicit consent from the data subject or processing necessary for certain purposes, such as healthcare or employment law. Additionally, high-risk processing under GDPR, such as large-scale use of innovative technologies, often necessitates Data Protection Impact Assessments (DPIAs) to mitigate risks to individuals' data privacy rights and freedoms.

Therefore, with nearly all highly regulated AI systems having a strong privacy component, managing these AI systems have not only a strong AI Act impact, but also a major GDPR impact. Managing these requirements together is therefore key. Involving and leveraging the expertise of a privacy professional will be pivotal in managing compliance for high-risk AI systems.

THE ROLE OF PRIVACY PROFESSIONALS IN GOVERNING AI

Leveraging experience

Over the past 6 years, since the GDPR came into force on May25, 2018, privacy professionals have been working on various aspects to ensure compliance and protect individual's privacy rights. Many of these experiences are valuable for AI Act compliance.

Even where privacy professionals within your organization are not directly responsible for governing AI-based systems, their involvement in the AI system lifecycle is likely to be important, given that many AI systems will also process personal data. Establishing clear links between the relevant stakeholders will help to ensure comprehensive governance of AI systems. In addition, leveraging the experience of privacy professionals in working towards compliance with EU regulations can be very beneficial in working towards compliance with the AI Act.

Some of these experiences that can support in AI Act compliance include:

Setting up and executing an organization-wide Compliance Program: Privacy professionals have been working with their organizations towards GDPR compliance. This involved understanding and interpreting the regulation itself, practical implementation, and managing stakeholders across the business. Unlike some other compliance programs, GDPR compliance – much like AI Act compliance – is inherently multidisciplinary. This complexity demands significant stakeholder management and coordination, which can be quite challenging. As a result, the experience and networks gained through GDPR compliance can be highly valuable when establishing an AI Act compliance project. Additionally, experience in interpreting and applying EU regulations is invaluable when determining how the AI Act applies to your organization and its impact on data processing practices.

Data Protection Impact Assessments (DPIAs): Conducting DPIAs for high-risk processing activities has become a regular part of their work. This involves assessing the potential risks to individuals' rights and freedoms and implementing measures to mitigate these risks. The AI Act also has requirements for risk assessments, which we will address in more detail in the next section.

Vendor Management: Assessing and managing the data protection practices of vendors and third parties to ensure they are in line with GDPR requirements. They've been evaluating and monitoring third-party vendors and service providers to ensure they comply with GDPR requirements when processing personal data on behalf of the organization. This includes reviewing contracts, conducting due diligence, and implementing appropriate safeguards. Managing vendors in the AI landscape is critical, especially as many organizations deploy third-party AI systems.

Data Mapping and Inventory: Privacy professionals have been maintaining detailed records of data processing activities as required by the GDPR. They've been working on creating data maps and inventories to identify the types of personal data collected, processed, and stored by the organization, as well as the purposes and legal bases for processing. Having a clear landscape of data held across the organization, makes it possible to identify AI systems that process personal data, and are therefore subject to GDPR. In addition, creating an AI systems registry is an important first step in AI Governance ([KPMG23]). This should be kept separate from an Article 30 registry, though the connection between the two should be made, i.e. it should be clear where data processes use a specific AI system. Depending on the governance structures of an organization, it may be possible to include the AI systems register within an

Asset register, as an AI system is a digital asset. It also enables transparency and explainability, as the data lineage is tracked. Data lineage refers to the life cycle of data, from its origins to how it has moved, processed, and transformed over time. It provides visibility while simplifying the ability to trace errors back to the root cause.

Data Minimization and Retention: Organizations must ensure that they collect and process only the minimum amount of personal data necessary for the specific purpose for which it is being processed. Privacy professionals have been identifying and supporting data minimization opportunities. The more data you possess, the greater your responsibility becomes. And once you have it, you need to be sure to manage it wisely. Data should also only be held for as long as required for processing, and in some cases has legal retention periods associated (e.g. in connection to national laws regarding HR/payroll records). Ensuring that the data used in AI systems is current and limited to what is necessary for its intended purpose is crucial for maintaining the quality of the AI system. Outdated data can compromise the accuracy and reliability of the results.

Awareness and Training: Raising awareness about data protection within the organization and providing necessary training to employees. Privacy professionals have been providing training and raising awareness among employees about their obligations under the GDPR, as well as the importance of data protection and privacy best practices. With new regulations and new obligations, your staff needs to be made aware of any additional or adjusted practices for compliance. The AI Act mandates that providers and deployers of AI systems have ensured that their staff have a sufficient level of AI literacy, likely requiring training, and awareness programs to facilitate and meet this requirement (Article 4). Make sure you use these compliance-based training skills of privacy professionals and programs to support staff members in doing the right thing with AI.

In the following section we will unpack several of these considerations, diving into the privacy practices that have an impact on AI Act compliance.

PRIVACY PRACTICES TO UNDERPIN AI ACT COMPLIANCE

Managing sensitive personal data

Under the GDPR, "special categories of personal data" are subject to stricter and more specific requirements for protection. As explored previously, this category of data is more likely to be present in high-risk AI systems. The GDPR defines special categories of personal data as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. Organizations must understand where they hold and process special categories of personal data, to ensure the correct handling of this data.

In most cases, processing sensitive personal data requires explicit consent from the data subject, unless another lawful basis applies. This means that consent must be freely given, specific, informed, and clearly expressed without any ambiguity. Additionally, the data subject must be able to withdraw his or her consent at any time. Maintaining accurate records of the types of data held, and on what basis, will enable privacy rights to be maintained, while holding personal data within AI systems.

Data Protection Impact Assessments, Fundamental Rights Impact Assessments & Conformity Assessments

Under the GDPR, the key assessment mandated is the Data Protection Impact Assessment (DPIAs). These assessments are compulsory when data processing operations are likely to pose a high risk to the rights and freedoms of individuals, particularly when sensitive personal data is involved. DPIAs aid organizations in identifying and mitigating risks associated with personal data processing. There are nine criteria to consider if a process is likely to result in high risk, including evaluations or scoring, automated decision making, systematic monitoring, sensitive data processing, large-scale data processing, matching or combining datasets, data concerning vulnerable subjects, innovative use or application of new technologies or organizational solutions, and processing that prevents individuals from exercising a right or using a service or a contract.

In the context of AI technologies, several of these criteria can apply as a matter of course, as they often involve large datasets, combining datasets, and some degree of evaluation and automated decision-making. They also

often represent the application of a new technology or solution. Meeting two of these criteria should generally trigger a DPIA, but even one could be sufficient.

Under the EU AI Act, there are two main assessments: the Conformity Assessment and the Fundamental Rights Impact Assessment, both of which are for high-risk AI systems.

Conformity Assessment (Article 43): Is mandated to ensure compliance with requirements for developing high-risk AI systems. This process should be conducted before the high-risk AI system is placed on the market or made available, or when substantial modifications elevate an AI system to high-risk status. There are two types of Conformity Assessment; the self-assessment based on internal controls, or the third party assessment which has to be assessed by an independent, approved body.

The Conformity Assessment needs to cover:
- Risk management system
- Data governance
- Technical documentation
- Record keeping
- Transparency and provision of information
- Human oversight
- Accuracy, robustness, and cybersecurity

Fundamental Rights Impact Assessment (Article 27): Is mandated with the aim to understand the impact of a high-risk system on fundamental rights, including privacy. It should be conducted prior to deploying a high-risk system, where the system is deployed by public bodies, or private entities providing public services, or by deployers of AI systems for evaluating creditworthiness, or risk assessments and pricing adjustment in life and health insurance.

In the Netherlands, the Ministry of the Interior and Kingdom Relations published an FRAIA – Fundamental Rights and Algorithms Impact Assessment, which can provide a helpful starting point in developing and performing such an assessment ([Gov21]).

With both the Conformity Assessment and the Fundamental Rights Impact Assessment, there will be overlap with the Data Protection Impact Assessment. By mapping the content of these assessments, and integrating, where possible, into the same process, organizations can avoid duplication of efforts.

Ultimately, the foundation to understanding which assessments you are required to conduct, is to understand your role (deployer, etc.) and the exact scope and purpose of your AI system, along with its risk rating.

PRIVACY REGULATORS AND AI

Privacy regulators play a pivotal role in ensuring compliance with the AI Act, particularly in safeguarding the rights and freedoms of individuals in the context of AI systems. While the AI Act primarily focuses on regulating AI systems, privacy regulators have a vested interest in its implementation due to its implications for data protection and privacy. The European Data Protection Board (EDPB) adopted a statement that "DPAs already have experience and expertise when dealing with the impact of AI on fundamental rights, in particular the right to protection of personal data, and should therefore be designated as Market Surveillance Authorities (MSAs) in a number of cases" ([EDPB24]).

In the Netherlands, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) has also been designated as the national coordinating authority for risk signaling, advice, and collaboration in the supervision on AI and algorithms since early 2023. This highlights the strong interconnectedness of governance between these two areas. In its second AI and Algorithmic Risks Report Netherlands ([Autor24]), the AP highlighted the urgent need for better risk management and incident monitoring. The advance of generative AI puts additional pressure on the development of effective safeguards.

The Dutch DPA have already had algorithms and AI-based systems in their sights for some time before the AI Act was adopted. In December 2021, the Dutch Data Protection Authority (DPA) imposed a fine of 3.75 million euros on the Dutch Tax and Customs Administration related to a GDPR violation for processing the nationality of applicants by a ML algorithm in a discriminatory manner[1]. The algorithm had identified double citizenship systematically as high-risk, leading to marking claims by those individuals more likely as fraudulent.

Overall, privacy regulators play a central role in ensuring that AI systems comply with data protection regulations and uphold individuals' privacy rights and freedoms. Their oversight, enforcement, guidance, and collaboration efforts contribute to achieving AI Act compliance and fostering trust in AI technologies.

1 The Dutch privacy regulator based its conclusions for the fine partly on the KPMG report on the FSV system (Fraude Signalering Voorziening), whereby the fraud risk selection algorithms resulted in a discriminatory "black list". The Dutch DPA concluded in line with the KPMG report that key privacy controls within and around the FSV system were non-compliant with all six major regulatory privacy principles (Article 5 GDPR, see further: https://www.edpb.europa.eu/news/national-news/2022/tax-administration-fined-fraud-black-list_en, and in Dutch:https://www.accountancyvanmorgen.nl/2020/07/11/bevindingen-kpmg-over-fiscus-ernstig-meer-fraudesystemen-uitgeschakeld/).

LOOKING AHEAD

International initiatives: Just like with the GDPR, which was a catalyst for similar privacy regulations to be implemented across the world, the same can be expected with the AI Act. Already many countries are publishing their AI strategies, and some are already working towards new legislation, as is the case with Canada and the AI and Data Act, part of Bill C-27 ([IAPP24]). The next few years are likely to see more of these regulations and guidelines, which will require organizations to account for potential nuance in their compliance.

AI audits: Although AI audits as such are not a requirement under the AI Act, they are useful tool for understanding if compliance goals are being met. Having an external perspective on your governance mechanisms, and risk measures, can provide insight into possible improvements, and missed blind spots. Linked to this, are, of course, the conformity assessments required when developing high-risk AI systems (Article 43), which can be performed internally, or by a certified external provider. In the next issue of Compact, you can read a specific article on AI Assurance in more detail.

AILD – liability rules: The Artificial Intelligence Liability Directive (AILD) is a proposal by the European Commission to adapt non-contractual civil liability rules to artificial intelligence ([EC24]). The purpose of the AILD is to improve the functioning of the internal market by laying down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems.

Additional regulations: The regulatory landscape within the EU continues to develop as the EU implements its Digital Strategy, including the Digital Services Act and Digital Markets Act, as well as the NIS2 Directive and the Data Governance Act. Organizations should aim to proactively monitor regulatory developments, and map requirements across legislations, rather than taking a siloed approach. In this way, organizations can leverage existing processes and programs, rather than building new projects for each legislation.

CONCLUSION

While the AI Act represents a new compliance challenge for organizations, it also builds on more established regulations like the GDPR. Although complex, the scope of the AI Act is more limited than the GDPR, and for many organizations, is unlikely to represent as impactful an implementation challenge as the GDPR.

Using the experience gained from GDPR compliance programs can provide a springboard for AI Act compliance. In addition, given the prevalence of personal data within AI systems, and in particular high-risk AI systems, involving data protection experts at all stages of an AI system development is critical.

To effectively understand their obligations, organizations must first clearly identify the AI systems they use and their role in relation to each system. This includes determining whether these systems contain personal data – especially special categories of personal data – and then identifying which requirements apply under both the AI Act and GDPR. Only with this clarity will the full impact of AI Act compliance become evident.

APPENDIX: THE EIGHT TYPOLOGIES OF HIGH RISK AI SYSTEMS UNDER THE AI ACT

In the following section we have outlined the eight typologies of high-risk AI systems under the AI Act, and some of the anticipated privacy implications.

1. **Biometric Identification and Categorization:** Systems used for biometric identification and categorization of natural persons, such as facial recognition systems used for surveillance.
   Biometric identification systems process highly sensitive personal data, including facial features, fingerprints, or iris scans, which fall under the special category of biometric data outlined in GDPR Article 9. Processing of biometric data is considered high risk, generally requiring the organization to conduct a DPIA.
2. **Critical Infrastructure Management:** AI systems that manage and operate critical infrastructure, such as water, energy, and transport, where malfunction could lead to significant harm. As critical infrastructure management primarily focuses on operational safety and security, it is less likely that personal data plays a pivotal role in this typology.
3. **Educational and Vocational Training:** AI systems used in educational or vocational training that determine access to education or professional advancement, influencing an individual's educational and career opportunities.
   AI systems used in educational and vocational training are likely to process personal data, including performance metrics, learning styles, and career aspirations. Since these factors can significantly influence individuals' educational and career opportunities, their processing must adhere to GDPR principles. However, if the system processes special categories of data, such as information about disabilities or (mental) health conditions, it would be considered sensitive data under GDPR Article 9 and require

stricter safeguards. In addition, if there are aspects of automated decision making, the processing can be expected to require a DPIA.

4. **Employment, Workers Management, and Access to Self-employment:** Systems that assist with recruitment, manage employees, or assess individuals for self-employment opportunities, impacting employment prospects.
   Similar to systems related to educational and vocational training, systems involved in employment, workers management, and access to self-employment is likely to process a wide range of personal data, including resumes, employment history, and performance evaluations. Additionally, if the system processes special categories of data, such as health information or information about criminal convictions, it would require heightened privacy protections under GDPR Article 9.
5. **Essential Private and Public Services:** AI systems that determine access to essential services, including credit scoring systems that assess creditworthiness.
   AI systems determining access to essential services, such as credit scoring systems, process personal data that can significantly impact individuals' financial well-being and access to necessities. These systems may use special categories of personal data, such as racial or ethnic information, or health data. Additionally, if the system involves profiling and/or automated decision-making, it may trigger the need for a DPIA under GDPR Article 35.
6. **Law Enforcement:** AI systems used by law enforcement for risk assessment, evidence analysis, and predicting criminal activity, impacting justice and policing.
   AI systems used in law enforcement may process vast amounts of personal data. This includes sensitive personal data such as criminal records or racial or ethnic origin, which require stringent privacy protections under GDPR. Additionally, the extensive profiling and surveillance involved in law enforcement activities is likely to necessitate a DPIA under GDPR Article 35 to assess and mitigate privacy risks.
7. **Migration, Asylum, and Border Control Management:** Systems used to manage migration, asylum, and border control, including assessing the eligibility of individuals for asylum.
   Systems used in migration, asylum, and border control management process personal data related to individuals' race or ethnic origin, religious beliefs, and sexual orientation. Given the sensitive nature of this data and its potential impact on individuals' rights and freedoms, it requires strict adherence to GDPR principles. Additionally, the large-scale processing of such data or the use of innovative technologies may trigger the requirement for a DPIA under GDPR Article 35.
8. **Administration of Justice and Democratic Processes:** AI systems that assist in judicial decision-making or other significant democratic processes, affecting the fairness and transparency of these processes.
   AI systems assisting in judicial decision-making or democratic processes may process personal data related to legal proceedings, voter information, or political preferences. Additionally, if the system processes special categories of data, such as information about criminal convictions or political opinions, it would require heightened privacy protections under GDPR Article 9.

Given that nearly all highly regulated AI systems have a significant privacy component, managing these systems involves not only substantial AI Act implications but also a major GDPR impact. Coordinating these requirements is therefore crucial. Involving and leveraging the expertise of a privacy professional will be pivotal in managing compliance for high-risk AI systems.

References

[Autor24] Autoriteit Persoonsgegevens (Dutch Data Protection Authority). (2024). AI & Algorithmic Risks Report Netherlands 2023/2024. Retrieved from: https://www.autoriteitpersoonsgegevens.nl/en/documents/ai-algorithmic-risks-report-netherlands-winter-2023-2024

[EC24] European Commission. (2024). Liability Rules for Artificial Intelligence. Retrieved from: https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

[EDPB24] European Data Protection Board. (2024). EDPB Statement on the Role of DPAs in the AI Act. Retrieved from: https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

[Gov21] Government of the Netherlands. (2021). Impact Assessment of Fundamental Rights and Algorithms. Retrieved from: https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms

[IAPP24] International Association of Privacy Professionals. (2024). Global AI Law and Policy Tracker. Retrieved from: https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf

[KPMG23] KPMG. (2023). Beyond Transparency: Harnessing Algorithm Registries for Effective Algorithm Governance. Retrieved from: https://www.compact.nl/articles/beyondtransparency-harnessing-algorithm-registries-for-effective-algorithm-governance/

[KPMG24] KPMG. (2024). Artificial Intelligence and the EU AI Act. Retrieved from: https://kpmg.com/ch/en/insights/technology/artificial-intelligence-eu-ai-act.html

About the authors

Stephan Idema is Director at KPMG Cyber & Privacy. He leads the Data Privacy team at KPMG and has been with KPMG for over 12 years. Stephan has a broad focus on compliance topics regarding digital legislations with a specific interest in privacy laws and AI regulation(s).

Daniela Gonzalez Riedel is Manager at KPMG Cyber & Privacy. She is an experienced privacy manager, working across KPMG NL & UK for over 7 years. She is primarily focused on translating (privacy related) legislative requirements into practical implementations, that enable businesses to innovate without compromising on compliance.