

## Privacy and AI – CCIA Europe's Recommendations

# Navigating the intersection of GDPR and AI: The need for a practical roadmap

April 2025

The rapid advancement of digital technologies presents both significant opportunities and challenges, especially at the intersection of different regulatory environments, such as the European Union's frameworks for data protection and artificial intelligence (AI).

As EU Member States and authorities prepare to streamline the AI Act and the General Data Protection Regulation (GDPR) – aiming to reduce redundancies and simplify compliance and enforcement – the Computer & Communications Industry Association (CCIA Europe) offers the following recommendations.

## I. Establish a framework for coherent application and cross-regulatory cooperation

*Effective implementation of the GDPR and AI Act requires a structured approach to ensure consistency and promote strong cooperation between competent authorities under both frameworks.*

### Recommendations:

1. Develop joint guidance and ensure appropriate consultation
2. Enhance inter-authority coordination
3. Establish coordinated protocols for investigation and enforcement

## II. Streamline governance for dual compliance

*Providers and deployers of AI systems often struggle with overlapping documentation and governance requirements. The EU must streamline these obligations to avoid adding unnecessary administrative burdens that divert resources from innovation.*

### Recommendations:

4. Leverage GDPR assessments for AI Act compliance and develop joint resources
5. Review and adapt already existing guidance
6. Promote interoperability of documentation standards

## III. Adopt risk-based and contextual interpretation

*Several core GDPR principles pose unique challenges for AI development and deployment. This is why the EU should adopt a more flexible, risk-based, and contextual interpretation.*

### Recommendations:

7. Follow a pragmatic interpretation of legal bases for special category data
8. Adopt a contextual application of the data minimisation principle
9. Maintain a risk-based approach to purpose specification and accuracy

## Introduction

The rapid advancement and growing integration of artificial intelligence (AI) technologies across various sectors presents both significant opportunities and complex challenges, particularly at the intersection with existing data protection rules.

The General Data Protection Regulation (GDPR) has long established a comprehensive framework for the processing of personal data within the European Union. With the recent adoption of the AI Act a new layer of harmonised rules specifically addressing AI systems has been added. This places the need to effectively navigate the interaction between these two critical legal frameworks at the forefront of regulatory and industry discussions today.

For this convergence to succeed, careful consideration is essential to ensure a coherent and effective legal framework that fosters AI innovation and upholds data protection rights.

Key challenges include defining the scope of personal data in AI systems, identifying appropriate legal bases for data processing, managing special category data, and adhering to the principles of data minimisation, purpose specification, and accuracy.

These challenges in achieving coherent application of both regulations have already been recognised by competent national authorities and supervisory data protection authorities. Indeed, striking the right balance is crucial to avoid stifling technological progress while maintaining high data protection standards.

In response to these complexities, the Computer & Communications Industry Association (CCIA Europe) proposes three key recommendations aimed at streamlining and improving the application of both the GDPR and the AI Act:

- I. Establish a framework for coherent application and cross-regulatory cooperation
- II. Streamline governance for dual compliance
- III. Adopt risk-based and contextual interpretation

By addressing the need for enhanced cooperation, streamlined compliance processes, and a contextual interpretation of key GDPR principles, these recommendations strive to balance responsible AI innovation with robust data protection in the EU.

## I. Establish a framework for coherent application and cross-regulatory cooperation

*Effective implementation of the GDPR and AI Act requires a structured approach to ensure consistency and promote strong cooperation between competent authorities under both frameworks.*

The distinct scope, definitions, and enforcement mechanisms of both the GDPR and AI Act present challenges that, if unaddressed, will lead to inconsistent enforcement – as well as creating uncertainty for business and hindering innovation.

### 1. Develop joint guidance and ensure appropriate consultation

Authorities must collaboratively develop shared guidelines on key areas of overlap between the GDPR and recently enacted legislation – such as the AI Act and sector-specific pieces (e.g. Data Act, Platform Work Directive, cybersecurity rules, etc). By way of example, the concept of ‘automated decision-making’ is defined in different ways in Article 22 of the GDPR, Article 86 of the AI Act, and Articles 9-11 of the Platform Work Directive, thus creating overlapping requirements and raising legal uncertainty. Joint guidance will allow for simplification and be instrumental to fostering a consistent understanding and application of both regulations, thereby reducing uncertainty for businesses.

CCIA Europe believes that all AI-related guidance documents issued by national authorities and relevant EU bodies – including the EU’s AI Office and the European Data Protection Board (EDPB) – should be subject to mandatory public consultation periods.

Such an inclusive approach will ensure that the perspectives of authorities, civil society, industry, and other stakeholders are duly considered, leading to more practical, effective, and well-informed implementation of the rules. Once finalised, these guidance documents should also be used as a metric to monitor the effectiveness of the implementation phase and the transposition of EU legislation into national law, where applicable.

### 2. Enhance inter-authority coordination

Having a consistent interpretation of the rules across the EU is essential for AI innovation. Currently, this poses challenges given the diversity of enforcement authorities when it comes to EU legislation – ranging from data protection to labour issues, or cybersecurity authorities with competences differing depending on national laws.

To avoid inconsistent or diverging interpretations of EU rules, authorities at both the EU and national levels should formalise their coordination and information sharing, for example by establishing a forum of digital regulators. This forum could serve as a central hub for information sharing, coordination on shared issues, alignment on policies and legal interpretations concerning AI and privacy, and establishing a leading authority in case of overlaps across the landscape of enforcers. The ultimate goal should be avoiding gaps and duplication of enforcement and compliance efforts.

The European Data Protection Supervisor’s (EDPS) proposal for a ‘Digital Clearinghouse’ offers a valuable model for such a structure and deserves serious consideration by Member

States.<sup>1</sup> Further, such a proposal aligns with the EDPB's role in ensuring the consistent application of the GDPR throughout the European Economic Area, a role that will be crucial in navigating the complexities of AI technologies.

### 3. Establish coordinated protocols for investigation and enforcement

To guarantee a harmonised approach, CCIA Europe suggests establishing clear protocols for joint investigations for cases that potentially involve violations of both the GDPR and the AI Act. Such an approach would prevent duplication of efforts, ensure coherence and consistency in enforcement, and streamline the overall regulatory and compliance processes.

Data protection authorities (DPAs) and competent authorities under the AI Act would need to work in tandem to address the multifaceted challenges posed by AI systems that process personal data. Moreover, with new digital legislation continuing to be implemented, it is crucial to maintain the 'one-stop-shop mechanism' for all EU and national legislation that involves data processing. This key GDPR principle is a pillar for consistency and harmonisation in enforcement. Upholding it is crucial to ensure harmonisation, legal certainty, and predictable oversight – in particular when it comes to cross-border operators.

The EU must therefore avoid any scenario in which companies face diverging demands from different Member States on the same issue. Because this would ultimately undermine EU competitiveness when it comes to technological advancements.

Sufficient means are also necessary to guarantee that enforcers have the necessary level of technical, economic, and scientific expertise. Joint training programmes for regulators – from both the data protection and AI domains – should be developed and implemented, in collaboration with industry and taking into account the diversity of expert knowledge required. In CCIA's view, these initiatives would help foster a shared understanding of the technical and legal complexities inherent in AI and promote smoother collaboration between regulatory bodies.

## II. Streamline governance for dual compliance

*Providers and deployers of AI systems often struggle with overlapping documentation and governance requirements. The EU must streamline these obligations to avoid adding unnecessary administrative burdens that divert resources from innovation.*

### 5. Leverage GDPR assessments for AI Act compliance and develop joint resources

To assist players of all sizes to navigate the regulatory maze, CCIA Europe believes that the EU institutions should actively explore opportunities to simplify overlapping requirements and leverage existing GDPR-compliance mechanisms to fulfill relevant obligations within all recently enacted digital legislation. This should cover anything from cybersecurity to labour or content moderation rules, and especially those provisions that relate to data.

<sup>1</sup> European Data Protection Supervisor's proposal to establish a Digital Clearinghouse 2.0. Concept note available [here](#).

For instance, documentation of personal data processing activities, risk assessments, and mitigation measures should be primarily covered within the GDPR-mandated Legitimate Interest Assessments (LIAs) and Data Protection Impact Assessments (DPIAs). This documentation should not be replicated in other frameworks, such as in the technical documentation of general-purpose AI (GPAI) models and high-risk AI systems under the AI Act, which will only add a new layer of complexity to the compliance burden for business.

Moreover, regulatory authorities should collaborate on the development of joint resources (such as FAQs, checklists, guidance materials) that specifically address the overlap in documentation and governance requirements. These resources would provide clarity and practical support to AI providers and deployers alike.

## 6. Review and adapt existing GDPR guidance

Existing guidance on DPIAs and LIAs should be reviewed and updated to explicitly reflect how these assessments can serve as a foundation for building a more comprehensive risk-management system that addresses both GDPR and AI Act requirements.

CCIA Europe considers that the aim should be to create a streamlined and integrated approach to documentation that promotes compliance without imposing unnecessary administrative costs or regulatory duplication. This could involve developing templates or frameworks that allow for unified assessment, covering key aspects of both regulations.

## 7. Promote interoperability of documentation standards

To streamline compliance for businesses of all sizes and capabilities, CCIA Europe believes efforts should be made to promote the interoperability of documentation formats and standards required under both the GDPR and the AI Act. This would facilitate the reuse of information and reduce the need for preparing multiple, similar documents.

By doing so, the EU can foster a more efficient and less burdensome compliance environment, allowing AI developers and deployers to focus on innovation while still adhering to the essential requirements of both Regulations. This streamlined approach will also help foster a thriving and responsible AI ecosystem in Europe.

## III. Adopt risk-based and contextual interpretation

*Several core GDPR principles pose unique challenges for AI development and deployment. This is why the EU should adopt a more flexible, risk-based, and contextual interpretation.*

The interpretation of a number of core principles in the GDPR, including the processing of special category data, data minimisation, purpose specification, and accuracy can present challenges when discussing AI development and deployment – particularly for GPAI models, as they often require the processing of vast amounts of data.<sup>2</sup> These challenges are not limited to the development of AI, but also raise significant challenges for deployers integrating and rolling out AI in complex operational settings. In order to guarantee AI

<sup>2</sup> Paper on ‘AI Hallucinations and Data Subject Rights under the GDPR: Regulatory Perspectives and Industry Responses’ by Theodore Christakis, available [here](#).

innovation and adoption, while respecting data protection rules, a flexible approach is urgently required.

## 9. Follow a pragmatic interpretation of legal bases for special category data

Enabling AI models to be properly trained is crucial for the EU to foster innovation and stay on par with global technological advancements. In this context, the EDPB should develop guidelines that inform a more pragmatic interpretation of Article 9 of the GDPR, concerning the processing of special category data for AI development. This could involve broadening the scope of applicable legal bases under Article 9(2), such as exploring the relevance of “scientific research” (Art. 9(2)(j)) or “substantial public interest” (Art. 9(2)(g)) for AI development and deployment, which would provide a more comprehensive framework for lawful processing of special categories of data.<sup>3</sup> In addition, the use of privacy-enhancing technologies (PETs) to minimise privacy risks when processing such data should be encouraged.

CCIA Europe believes that extending the AI Act’s provision allowing for the processing of special categories of data to detect and correct bias should be extended to all AI systems and GPAI models, not only just the ones categorised as ‘high-risk’. This would recognise the importance of detecting and correcting bias for all AI systems, irrespective of their risk classification.

## 10. Adopt a contextual application of the data minimisation principle

CCIA Europe considers it necessary to move beyond a purely quantitative and restrictive approach to data minimisation.<sup>4</sup> The interpretation of “necessary” data in the context of AI should recognise the large data volumes essential for robust model training, high-quality outputs, and bias mitigation – as acknowledged in Article 10(3) of the AI Act.

A flexible, contextual interpretation that is proportionate to the risks and benefits of AI is crucial. This should consider dynamic data minimisation techniques (such as differential privacy, on-the-fly anonymisation, and selective data processing) as potential mechanisms to balance data protection requirements with system functionality.

## 11. Maintain a risk-based approach to purpose specification and accuracy

Given the inherent nature of GPAI models, which can be used for a wide variety of evolving applications and have no specific purpose, a rigid interpretation of the purpose specification principle under the GDPR may stifle innovation. To avoid such a contradiction, the training of a GPAI model should be seen as a legitimate purpose in itself, subject to existing GDPR rules and safeguards.

Similarly, when assessing accuracy under the GDPR in the context of AI-generated outputs, the focus should be on reliability that is appropriate in a given context and on mitigating inaccuracies that could be harmful through transparency mechanisms and user empowerment (including disclaimers, fact-checking features, etc). The articulation of an

<sup>3</sup> Paper on ‘Generative AI in EU Law: Liability, privacy, intellectual property and cybersecurity’ by Claudio Novelli et al, available [here](#).

<sup>4</sup> As also acknowledged by the European Data Protection Supervisor in their paper ‘Generative AI and the EUDPR’ of 3 June 2024, available [here](#).

appropriate level of accuracy in the AI Act (Article 15(1)) and its emphasis on intended purpose (Art. 10(3)) should guide a pragmatic approach under the GDPR.

In this context, the Hamburg DPA's focus on the outputs of AI systems and the UK ICO's emphasis on the purpose and context of AI use offer valuable perspectives that could be taken into account.<sup>5</sup>

By embracing a risk-based and contextual interpretation of key GDPR principles, regulators can create a more enabling environment for responsible AI innovation and adoption in Europe. It would ensure that the pursuit of technological advancement is balanced with the fundamental right to data protection. This nuanced approach acknowledges the unique characteristics of AI technologies and the need for pragmatic solutions.

## Conclusion

Navigating the intersection of data protection and AI frameworks is a complex but essential task for the European Union. CCIA Europe's recommendations outlined in this document offer concrete steps towards achieving a more harmonised and effective regulatory environment.

Adequately and consistently applying both regulations will be crucial to ensure that the EU can harness the transformative potential of AI while upholding its commitment to the fundamental right to data protection.

Without a doubt, the path forward will require ongoing dialogue and collaboration among regulators, industry stakeholders, civil society, and researchers. As AI technologies continue to quickly evolve, so must the regulatory approaches. The guidance provided by DPAs, such as the Hamburg DPA's focus on AI outputs and the ICO's emphasis on purpose and transparency – along with the EDPB's efforts to provide clarity on key issues such as anonymisation and legitimate interest<sup>6</sup> – are vital in shaping a pragmatic and innovation-friendly application of the GDPR in the age of AI.

Ultimately, the goal is to align EU privacy laws with the realities of AI development and deployment. Both regulations need to work together in practice to foster responsible AI innovation within a strong framework for data protection. This requires a willingness to adapt existing interpretations, embrace risk-based approaches, and prioritise practical solutions that reduce unnecessary burdens while ensuring meaningful safeguards for individuals.

The future success of AI in the European Union hinges on its ability to create a regulatory landscape that is both robust and agile, capable of navigating the complexities of AI technologies while remaining committed to protecting the rights and freedoms of individuals.

<sup>5</sup> Discussion paper 'Large Language Models and Personal Data', from the Hamburg Commissioner for Data protection and freedom of information, available [here](#) and 'Generative AI third call for evidence: accuracy of training data and model outputs' from the UK's Information Commissioner's Office, available [here](#).

<sup>6</sup> European Data Protection Board's Opinion 28/2024 on 'certain data protection aspects related to the processing of personal data in the context of AI models', available [here](#).

## About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit [ccianet.eu](http://ccianet.eu), [x.com/CCIAeurope](https://x.com/CCIAeurope), or [linkedin.com/showcase/cciaeurope](https://linkedin.com/showcase/cciaeurope) to learn more.

**For more information, please contact:**

CCIA Europe's Head of Communications, Kasper Peters: [kpeters@ccianet.org](mailto:kpeters@ccianet.org)