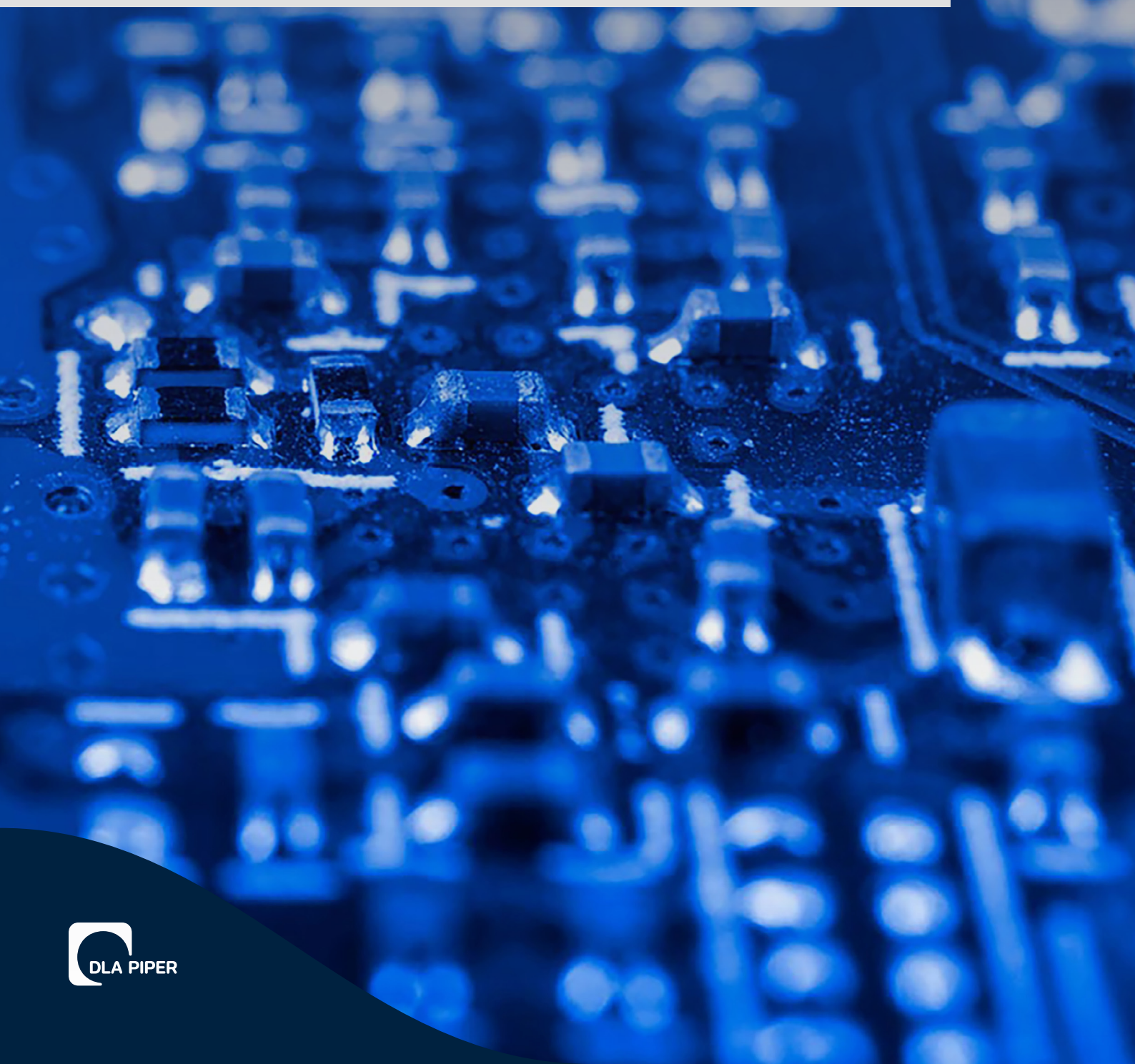
ISSUE N.09 | MAY 2025

Diritto intelligente

In this issue



DLA PIPER

Contents

Editorial

Welcome to the latest edition of Diritto Intelligente, our AI law journal dedicated to exploring cutting-edge legal developments in the rapidly evolving domain of artificial intelligence.

In this issue, Giacomo Lusardi offers an insightful examination of the updated Model Contractual Clauses for AI Procurement (MCC-AI) published by the European Commission. These clauses provide a practical and modular framework designed to assist sector entities in managing compliance risks associated with AI procurement, particularly focusing on transparency, risk management, accountability, and data governance – although private sector buyers my find inspiration too. Giacomo critically assesses the potential of MCC-AI to streamline negotiations and reduce legal uncertainties, highlighting their adaptability within broader contractual frameworks, yet cautioning about their effectiveness in markets dominated by large vendors and open-source AI solutions.

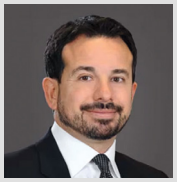
Then I address the emerging and highly sensitive issue of AI hallucinations. My analysis of recent cases in Italy and Canada, where generative AI tools inadvertently created fictitious legal citations, underscores the necessity for rigorous human oversight. I discuss the professional and ethical obligations of legal practitioners in the context of AI use, emphasizing the need for robust regulatory frameworks that preserve the accuracy, integrity, and reliability essential to legal practice.

Dorina Simaku explores the European Commission's targeted consultation on the implementation guidelines for the AI Act, particularly regarding General-Purpose AI (GPAI). She details the significant operational challenges these versatile technologies present and the importance of stakeholder engagement in shaping clear regulatory expectations. Dorina emphasizes the potential benefits of adhering to the forthcoming AI Code of Practice, which promises regulatory alignment and recognition of best practices.

Finally, Lara Mastrangelo analyzes the legal complexities surrounding AI-generated deepfakes, focusing on the legislative debates in the United States around the NO FAKES Act and EU regulations touching on the same topics. Lara highlights the pressing need to balance innovation and technological advancement with fundamental rights protection, particularly concerning personality rights and content authenticity.

And, as in each issue of Diritto Intelligente, you will find the insights on legal design from Deborah Paracchini and on legal tech from Tommaso Ricci.

We hope you find this issue engaging and informative, supporting your efforts to navigate the complex and dynamic world of AI law.



Giulio Coraggio
Location Head of the Italian Intellectual Property and Technology Department at DLA Piper

Model contractual clauses for AI procurement: How updated EU clauses help manage compliance risk

Author: *Giacomo Lusardi*

The European Commission has published the updated Model Contractual Clauses for AI Procurement (MCC-AI) to help public sector entities procuring AI comply with the provisions of the AI Act.

Originally introduced in September 2023, the clauses serve as a practical and modular tool designed to help both public buyers navigate the regulatory challenges associated with sourcing and providing of AI systems.

Purpose of the MCC-AI

The MCC-AI have been drafted for those looking to procure AI. While primarily aimed at public sector AI buyers, as we explore below, private sector AI customers may find them of use. They are designed to facilitate alignment with key regulatory requirements under the AI Act, particularly in areas like transparency, risk management, accountability, and data governance.

Adopting the MCC-AI allows organizations to:

- reduce legal uncertainty;
- demonstrate regulatory readiness;
- potentially streamline contractual negotiations.

Two-tiered approach based on risk level

The updated MCC-AI package includes two distinct versions:

- a full version for high-risk AI systems (AI systems intended to be used for emotion recognition, for recruiting or selecting of natural persons, or to evaluate the creditworthiness of natural persons);
- a light version for non-high-risk AI systems, which still ensures safeguards around key elements such as technical documentation and algorithmic transparency.

The package also includes an explanatory commentary offering guidance on how to tailor and integrate the clauses into existing contracts.

Usability for private sector operators

Although originally tailored for public procurement, the MCC-AI can also be adopted by private sector entities, with the necessary adaptations. AI systems procurers can incorporate these clauses into their contractual arrangements to align with emerging EU regulatory best practices.

This is especially valuable in today's evolving legal landscape, where AI regulations are still taking shape and efforts are being made in some quarters to achieve greater harmonization.

Especially in the case of private companies, the MCC-AI are not a static tool to be incorporated into contracts as they are but need to be contextualized and adapted to the specific supply and the relevant economic sector.

Structure and key content areas

The MCC-AI are not stand-alone contracts but are intended to be embedded in broader services agreements. They exclusively address AI-specific obligations under the AI Act and (importantly) do ***not*** cover general contractual matters such as intellectual property, payment terms, applicable law, or traditional contractual liability, which the company involved must also carefully regulate.

The clauses are structured around five key thematic areas:

- AI System Compliance – Identifying applicable legal and ethical standards for the AI solutions provided.
- Supplier Roles and Responsibilities – Defining transparency requirements, risk management obligations, and compliance duties.
- Data Governance – Establishing criteria regarding data ownership, usage, and oversight of datasets used in AI systems.
- Verifiability and Traceability – Implementing audit tools, documentation requirements, and system performance monitoring.
- Cost Allocation – Clarifying financial responsibilities related to system implementation and necessary adjustments.

To facilitate adoption, the MCC-AI also include technical annexes with sample use cases, data governance templates, and model compliance documentation.

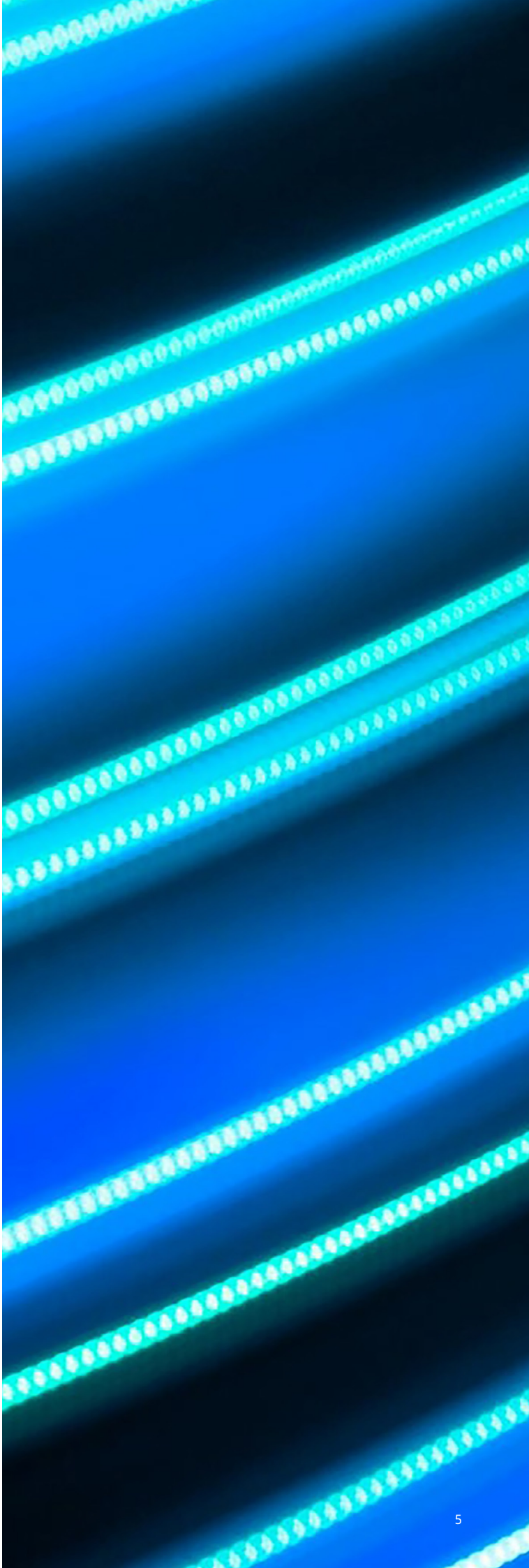
Why consider adoption?

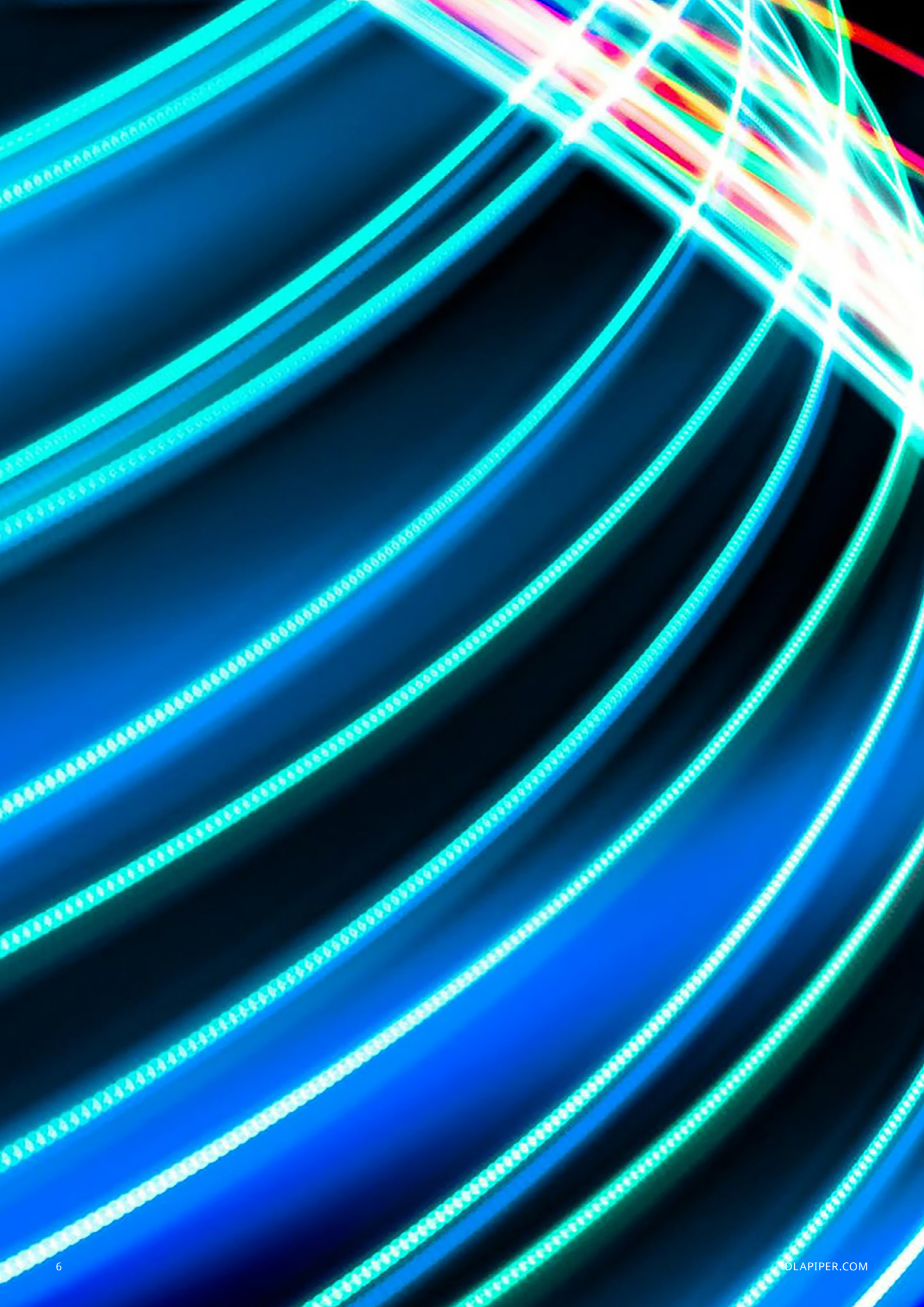
For AI purchasers, these clauses provide a legal and ethical safeguard, particularly in scenarios where AI applications might affect fundamental rights or public safety.

The modular design of the MCC-AI is intended to allow for seamless integration and adaptation into existing contractual frameworks, supporting consistent management across different procurement contexts while simplifying processes and helping prevent potential disputes.

Although they are not legally mandated for thse procuring AI (even in the public sector) the MCC-AI offer a valuable operational support to address the issue of contractual governance in supplying and procuring of AI systems.

The difficulty with MCC-AI adoption is that relatively few AI procurements are undertaken in circumstances where the balance of negotiating power rests with the buyer. In a world of AI subscriptions from large vendors, and increasing adoption of open source/open-weights AI subject to short-form standard licenses, it will be interesting to see whether the updated MCC-AI terms gain traction.





What happens when the AI hallucinates the courtroom?

Author: *Giulio Coraggio*

What happens when an artificial intelligence (AI) tool like ChatGPT invents a legal ruling—and that ruling ends up in a courtroom filing?

The cases on AI hallucinations in court in Italy and Canada

In the matter at hand, a lawyer submitted a defense brief in a trademark and copyright dispute that included citations from the Italian Supreme Court. Upon review, it emerged that these references were entirely fictitious—fabricated by ChatGPT, a generative AI model. The court acknowledged that the citations were produced without malicious intent, attributing the incident to the failure of the attorney to verify the accuracy of research conducted by a colleague using AI. As a result, a claim for aggravated liability under Article 96 of the Italian Code of Civil Procedure was dismissed for lack of demonstrable harm.

This episode is not isolated. In a separate case before the Supreme Court of British Columbia in Canada, a lawyer submitted two fabricated judgments generated by ChatGPT in a custody dispute. The lawyer admitted to using the tool without being aware of its limitations and was ordered to personally compensate the opposing party for the resulting procedural delays.

These cases are just the latest in a growing collection of cases across many jurisdictions where lawyers have been caught out relying AI which has imagined fictitious cases. They underscore a significant and growing concern: the risk of AI hallucinations—that is, the generation of plausible-sounding but entirely false information. While generative AI models have proven valuable for enhancing efficiency and supporting routine tasks, they lack the capacity to assess the factual or legal accuracy of their outputs. In legal contexts—where precision and accountability are paramount—this limitation presents serious professional and ethical implications.

The imperative of human oversight

As the legal sector increasingly explores the adoption of AI-driven tools, the importance of maintaining rigorous human oversight cannot be overstated. Legal professionals must carefully review and validate all AI-generated content, particularly when used in the context of legal submissions, opinions, or advice. The role of the lawyer remains indispensable in interpreting legal texts, assessing jurisprudence, and ensuring the accuracy and relevance of cited authorities.

The regulatory landscape: AI and the legal profession

The emergence of such incidents also prompts reflection on broader regulatory developments. Under the proposed EU AI Act, the use of generative AI in legal services may qualify as a high-risk application—particularly where it affects individuals' rights or legal obligations. In such cases, the deployment of AI tools must comply with stringent requirements concerning accuracy, traceability, and human oversight.

The submission of hallucinated case law—even if unintentional—could raise concerns not only for the individual legal practitioner but also for the law firm and the AI provider involved. To mitigate these risks, it is critical that legal AI solutions are designed with reliable, verifiable sources and deployed within robust risk management frameworks.

Conclusion

The integration of AI into legal practice is inevitable and, when implemented responsibly, can provide significant advantages. However, these recent cases serve as a cautionary reminder of the professional obligations that remain unchanged. The use of advanced technology must never compromise the duty of diligence, accuracy, and integrity that lies at the core of legal work.

Legal professionals, firms, and institutions must approach the adoption of AI with caution, transparency, and a clear understanding of the applicable legal and ethical standards. Only then can innovation serve as an enabler of progress—rather than a source of liability.

GPAI: European Commission launches targeted consultation on rules, obligations and implementation practices

Author: *Dorina Simaku*

The European Commission has launched a targeted consultation to support the development of Guidelines for implementing the AI Act, inviting all relevant stakeholders to submit their input via a survey until May 22, 2025.

Through this multi-stakeholder consultation, the Commission aims to gather operational and practical insights from General-Purpose AI (GPAI) providers, downstream AI system developers, researchers, public authorities, and other professionals. The goal is to support the development of Guidelines that facilitate the effective enforcement of Regulation (EU) 2024/1689 (AI Act).

Why is this consultation critical?

GPAI systems present unique regulatory challenges. Their versatility enables them to perform a wide range of tasks and be embedded into countless downstream applications. This creates significant grey areas in legal qualification and compliance obligations – a complexity compounded by the rapid evolution of AI technologies.

With GPAI-specific provisions set to apply from August 2, 2025, the Commission seeks to clarify several key issues:

- Refining the definition of "GPAI": establishing the scope of models falling under this classification.
- Providing accountability: identifying who holds responsibility in complex, layered development chains.
- Further defining "placing on the market": determining the precise moment a GPAI model is considered to have been made available.
- Calculating computational thresholds: defining how to measure computational resources used during model training, which may be relevant when determining whether a GPAI presents a systemic risk.
- Open-source exemptions: clarifying when and how regulatory exemptions apply.
- Code of Practice: outlining the benefits and commitments of adhering to the voluntary Code.

The role of the European AI office

The European AI Office, supported by the Joint Research Centre, will lead in drafting of these Guidelines. Although non-binding, they will serve as the Commission's official interpretative framework for the implementation of the AI Act, especially Articles 52–55. They will be a crucial reference point for operators seeking compliance.

Code of practice: Benefits of adhering

A central element of the consultation is the forthcoming AI Code of Practice, designed to support responsible GPAI development and use. The Commission asserts that participation in this Code will offer advantages for providers, including:

- increased trust: with non-signatories being expected to demonstrate AI Act compliance via other means, potentially with additional explanation;
- regulatory alignment: offering a structured path to meet AI Act obligations; and
- recognition of best practices: establishing operational standards at both EU and international levels.

The Code is intended to be fully aligned with the AI Act and will address key aspects such as documentation requirements, copyright risk management, and specific safeguards for models deemed to pose systemic risk (Articles 53 and 55).

What should developers and businesses know?

For organizations developing, modifying, or integrating GPAI models, this consultation is an opportunity to shape future regulatory expectations and seek clarity on their roles and responsibilities under the AI Act.

The consultation remains open until 22 May 2025, while the final Guidelines and Code of Practice are expected to be published between May and June 2025.

Final remarks

This initiative marks a pivotal moment in the EU's journey towards a coherent and operational AI regulatory framework. Rather than merely collecting opinions, the consultation is a participatory process – one that allows industry players to actively contribute to a future where innovation is matched by accountability. Engaging now means helping to define a legal environment built on clarity, cooperation, and mutual trust – the foundations for a trustworthy AI ecosystem in Europe.

Legal challenges of AI, deepfakes, and the NO FAKES Act

Author: *Lara Mastrangelo*

AI generated deepfakes create significant legal challenges regarding personality rights and content authenticity in the creative industry. The industry must balance technological innovation with protecting personality rights.

The US legal landscape: The NO FAKES Act

First introduced in 2023 and reintroduced in 2024 (having not made it through the legislative process initially), the federal NO FAKES Act—short for Nurture Originals, Foster Art, and Keep Entertainment Safe—is once again at the center of US legislative debate. Enjoying bipartisan support, the bill aims to establish a uniform legal framework to protect individuals' rights to their image and voice in the face of rapidly advancing generative AI technologies.

The latest version of the draft law, the result of months of negotiations with stakeholders from the tech and media sectors, seeks to curb the unauthorized use of deepfakes and digital replicas. It addresses the current patchwork of state-level protections, given that image and personality rights are pesently governed by state law, with no consistent federal standard. If passed, the NO FAKES Act would introduce a federal private right of action and set clearer rules for the removal of unlawful content.

Key legal measures in the NO FAKES Act

The latest version introduces essential legal protections and enforcement mechanisms:

- **Obligations for online services**: Platforms will not be held liable for hosting illegal digital replicas if they promptly remove the content upon receiving a valid notice and inform the uploader. However, platforms "designed or promoted" specifically to create deepfakes are excluded from these protections.
- **Investigation powers for rights holders**: Rights holders will be able to obtain, through a court order, identifying information of anonymous users who uploaded content in violation of image rights.
- **Stricter safe harbor conditions**: Service providers can only benefit from liability exemptions if they implement effective mechanisms for removing unlawful content and suspending repeat offenders.
- **Fingerprinting technologies**: Platforms will be required to adopt digital identification tools (such as cryptographic hashes) to prevent the re-uploading of content that has already been flagged and removed.
- **Expanded definition of "online service"**: The scope of the law is broadened to include search engines, ad networks, marketplaces, and cloud services, provided they register an agent with the Copyright Office.
- **Graduated penalty system**: Fines range from USD5,000 per violation up to USD750,000 per piece of content, targeting platforms that fail to show good faith efforts in complying with the law.
- **No proactive monitoring obligation**: In line with the DMCA, platforms are not required to actively monitor content but must act swiftly on valid notices in order to retain safe harbor protections.

Compared to earlier versions, the revamped NO FAKES Act has gained support from key players in the tech and entertainment industries, including major record labels and the Recording Industry Association. However, the bill continues to raise concerns among civil liberties groups, who fear it could impose overly restrictive limits on freedom of expression.

Italy's legal response: ANAD's stand on AI Deepfake

The reintroduction of the NO FAKES Act comes within a broader and increasingly sensitive context, particularly in sectors where the debate is heating up. One source of concern is the use of software for AI voice cloning and manipulation. For instance, such technology was recently used in the film *The Brutalist* to refine the Hungarian pronunciation of its two lead actors, altering their voices.

In this regard, ANAD – the Italian National Association of Voice Actors – has recently raised objections to the use of technologies capable of sampling actors' voices without their consent and outside clear and shared regulatory frameworks. The association has specifically called for the recognition of voice as a biometric datum, comparable to a fingerprint, to ensure the broadest possible protection.

Italy's dubbing industry is long-established and among the first to take regulatory steps. In fact, during the drafting of the new national collective bargaining agreement in June 2024, a specific clause was introduced to regulate the lawful (or unlawful) use of actors' voices by AI systems.

How the EU AI Act regulates deepfakes

The AI Act defines a "deep fake" in Article 3(60) as *"AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful."* and Article 50 of the AI Act introduces transparency obligations.

- **For providers**: Entities that develop AI systems capable of generating synthetic content (such as images, audio, or video) must ensure that outputs are marked in a machine-readable format as artificially generated or manipulated (Art. 50(2)).;
- **For deployers**: Organizations or individuals using such AI systems generating synthetic content that constitutes ca 'deepfake' are required to disclose that the content has been artificially generated or manipulated. This disclosure should be clear and provided at the latest upon the first interaction or exposure to the content

There are exceptions to this disclosure obligation which apply, among others, to

- **Artistic or satirical content**: If the AI-generated content is evidently part of an artistic, creative, satirical, or fictional work, the disclosure can be made in a manner that does not hinder the enjoyment or display of the work; and
- **Law enforcement use**: AI systems authorized by law for purposes such as crime detection or prevention may be exempt from certain transparency requirements

While deepfakes are generally categorized under "limited risk" AI systems, their classification can escalate to "high risk" if used in contexts that significantly impact individuals' rights or society, such as political manipulation or defamation. High-risk classification entails stricter regulatory requirements under the EU AI Act.

4. Balancing legal protections and innovation

In an era where faces and voices—especially those of public figures—are becoming valuable digital assets, their replication through artificial intelligence strikes a sensitive chord and involves a wide range of legal areas: from privacy to personality rights, from defamation to financial damages resulting from unauthorized use. It will therefore be crucial to strike a balance between creativity, innovation, and the protection of fundamental rights.

Legal design tricks

Trick #8: Write Clearly – Words Matter!

You have tested your solution? Great. Now it's time to simplify the language and make your documents speak... crystal clear!

Author: *Deborah Paracchini*

Why clarity really matters

Legal documents often speak a language few understand. Legal jargon is frequently perceived as obscure, overly technical, and reserved for insiders.

But an incomprehensible document is also an ineffective one.

Remember: Clarity makes the law accessible, builds trust, and simplifies your work.

Legal Design = clarity + accessibility

Legal Design promotes clarity and accessibility. A text is truly clear when the reader can find the information, understand it, and use it with ease.

- **Clarity** = no more useless legalese
- **Accessibility** = content that's understandable for everyone, not just lawyers

What is plain language?

According to the ISO plain language standard, a text is truly understandable when:

- It gives users what they need (relevance)
- It's easy to navigate (findability)
- It's immediately understandable (comprehensibility)
- It's easy to use (usability)

How to simplify legal language?

- Use simple, familiar words – avoid unnecessary technicalities
- Remove outdated or archaic terms ("*herein*", "*aforementioned*", "*shall*")
- Avoid unnecessary foreign terms or jargon
- Keep sentences short. One idea per sentence
- Explain difficult legal terms clearly – include definitions when needed
- Prefer the active voice ("*The company sends the invoice*") over passive ("*The invoice is sent by the company*")
- Replace negatives with positives where possible ("*not permitted*" → "*prohibited*")
- Speak directly to your reader with a friendly tone

Is your language truly readable? Run a readability test!

There are online tools that help you measure how easy your text is to read.

In Italian, the most widely used tool is the Gulpease Index, which considers sentence and word length.

In English, try the Flesch Reading Ease or Flesch-Kincaid Grade Level: they show how readable your text is, and for what education level.

Remember: If the score is low... it's time to rewrite!

Let's make an example!

Our usual client has tested their contract but... users still ask too many questions. So, the legal team decides to:

- Rewrite it using shorter sentences and active verbs
- Simplify definitions and clauses
- Eliminate legalese and clarify unclear parts

The result? More clarity, fewer emails, faster signature!

Did you know?

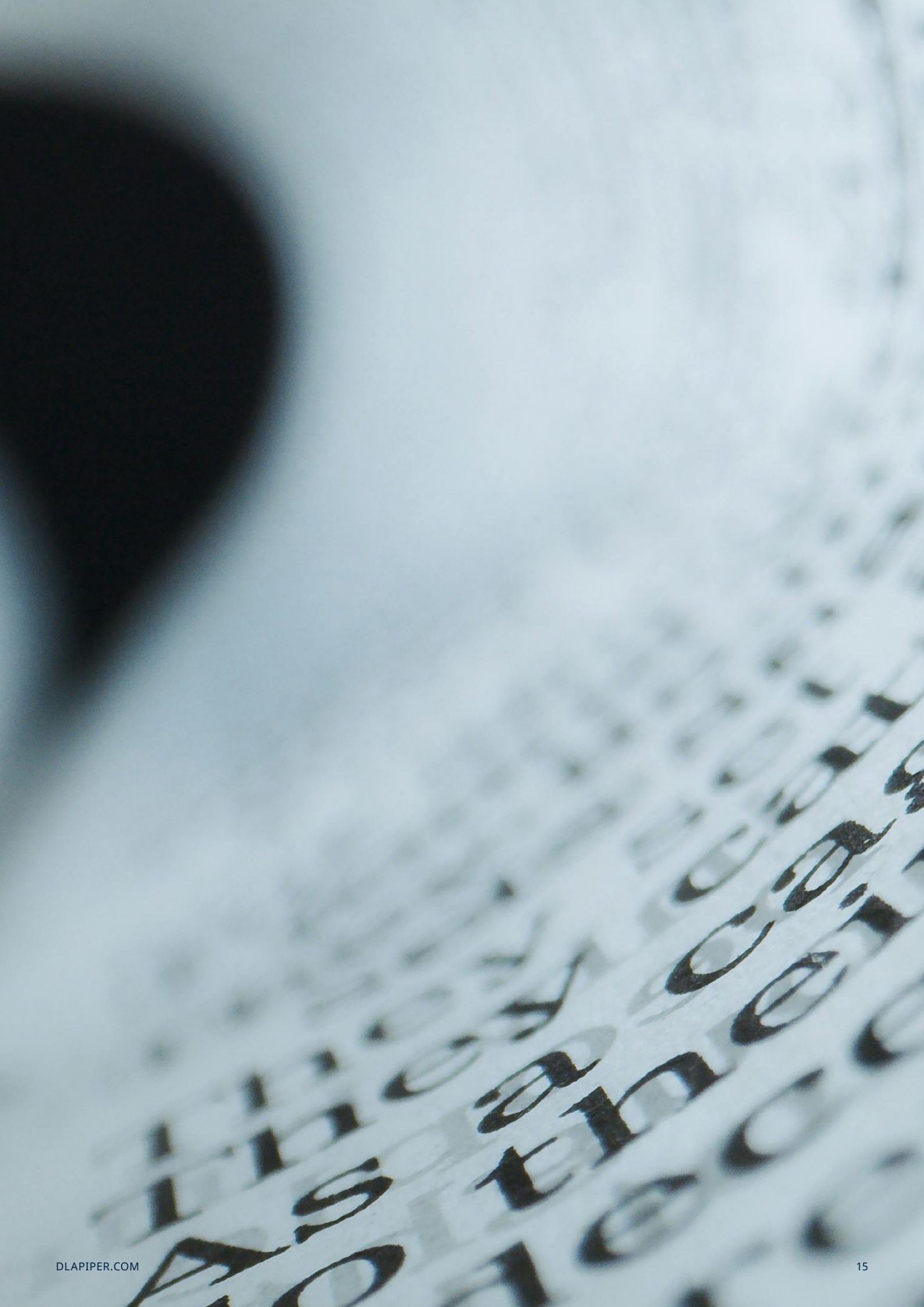
The ISO standard on plain language is the first ever to certify when a text is truly clear.

It was developed by experts from around the world to simplify legal, technical, and informational content.

Its motto? *Say what you mean. Mean what you say.*

What's next?

You've simplified the language... but how do you really design an effective legal document? **In the next episode of Legal Design Tricks, we will talk about information architecture –** because layout and structure matter, especially when it comes to contracts!



Legal tech bytes

Expert insights on the latest trends and innovations

Author: *Tommaso Ricci*

Build vs. Buy: strategic decision-making for legal AI solutions procurement

The legal technology landscape is rapidly changing as organizations look to harness AI capabilities. Legal departments face an important choice: build custom AI solutions or buy existing ones. This decision has significant impacts on efficiency, cost, and competitive advantage.

The current AI adoption landscape

According to the 2025 Thomson Reuters Generative AI in Professional Services Report, approximately 41% of legal professionals are now using publicly available AI tools, with an additional 17% utilizing industry-specific AI solutions. This represents substantial growth, with organization-wide AI usage nearly doubling over the past year to 22% in 2025, compared to just 12% in 2024.

Most significantly, 95% of legal professionals believe AI will be central to their organization's workflow within the next five years, despite only 13% reporting it as central today. This demonstrates a clear trajectory toward widespread integration, making the build vs. buy decision increasingly important. Here's a suggestion on a Methodology for Strategic Evaluation to help you compare the two options.

Phase 1: Needs assessment and use case prioritization

Before deciding whether to build or buy, legal departments must conduct a thorough assessment of their specific needs (we've discussed our suggested pain/opportunity assessment methodology in former episodes of Legal Tech Bytes):

1. **Volume and frequency analysis**: Identify high-volume, repetitive tasks that consume significant resources (document review, contract management, legal research)
2. **Complexity assessment**: Evaluate the technical complexity and domain specificity required
3. **Strategic alignment**: Determine how AI integration connects to broader organizational goals.

Phase 2: Comprehensive cost-benefit analysis

A holistic evaluation must consider both direct and indirect costs:

For building solutions:

- Initial development costs (internal or outsourced)
- Ongoing maintenance and updates
- Infrastructure requirements
- Training and implementation
- Opportunity costs of allocated resources

For buying solutions:

- Licensing expenses (subscription or one-time)
- Customization and integration costs
- Staff training requirements
- Vendor dependency risks
- Data migration and security concerns

Importantly, the Generative AI in Professional Services report reveals that only 20% of organizations are currently measuring ROI from their AI investments, while 59% are not measuring ROI at all. We've discussed our LegalTech ROI calculation methodology and tool in previous episodes, make sure to check it out.

Phase 3: Internal capability assessment

Legal departments must realistically evaluate their available resources:

- Technical expertise: Access (internal or external) to developers, data scientists, or IT staff with AI experience
- Domain knowledge: Ability to translate legal requirements into technical specifications
- Governance capabilities: Structures for managing complex technology projects
- Support capacity: Resources for ongoing maintenance and enhancement
- Time and budget, which can be quantified based on a reasonable forecast of the expected ROI and effective savings in the short/medium/long term depending on the purpose of the solution.

Phase 4: Security and compliance analysis

Data security and IP considerations are crucial as the processing activities performed by the legal function can involve highly confidential information of the company:

- Data residency requirements and jurisdictional constraints
- Access controls and authentication protocols
- Training data usage policies
- Regulatory compliance (e.g. GDPR + AI Act) and certifications which might be necessary

Decision framework: when to build vs. when to buy

Based on this, you might consider to

Build when:

- Your organization has highly specialized, unique requirements
- You possess valuable proprietary data that provides competitive advantage
- Data security and confidentiality are mission-critical concerns
- You have an established and trusted team with AI and legal domain expertise
- The solution represents a strategic differentiator

Buy when:

- You need standardized functionality (e.g., general legal research, basic contract review)
- Internal IT or data science resources are limited
- You require rapid implementation
- The total cost of ownership for an internal solution would significantly exceed licensing costs
- The solution requires continuous updates based on evolving regulations or case law

Hybrid approaches

As organizations mature in their AI adoption and are starting to realize which solutions have actually delivered the expected value after their build VS. buy decisions, many are finding a convenient third way in hybrid approaches:

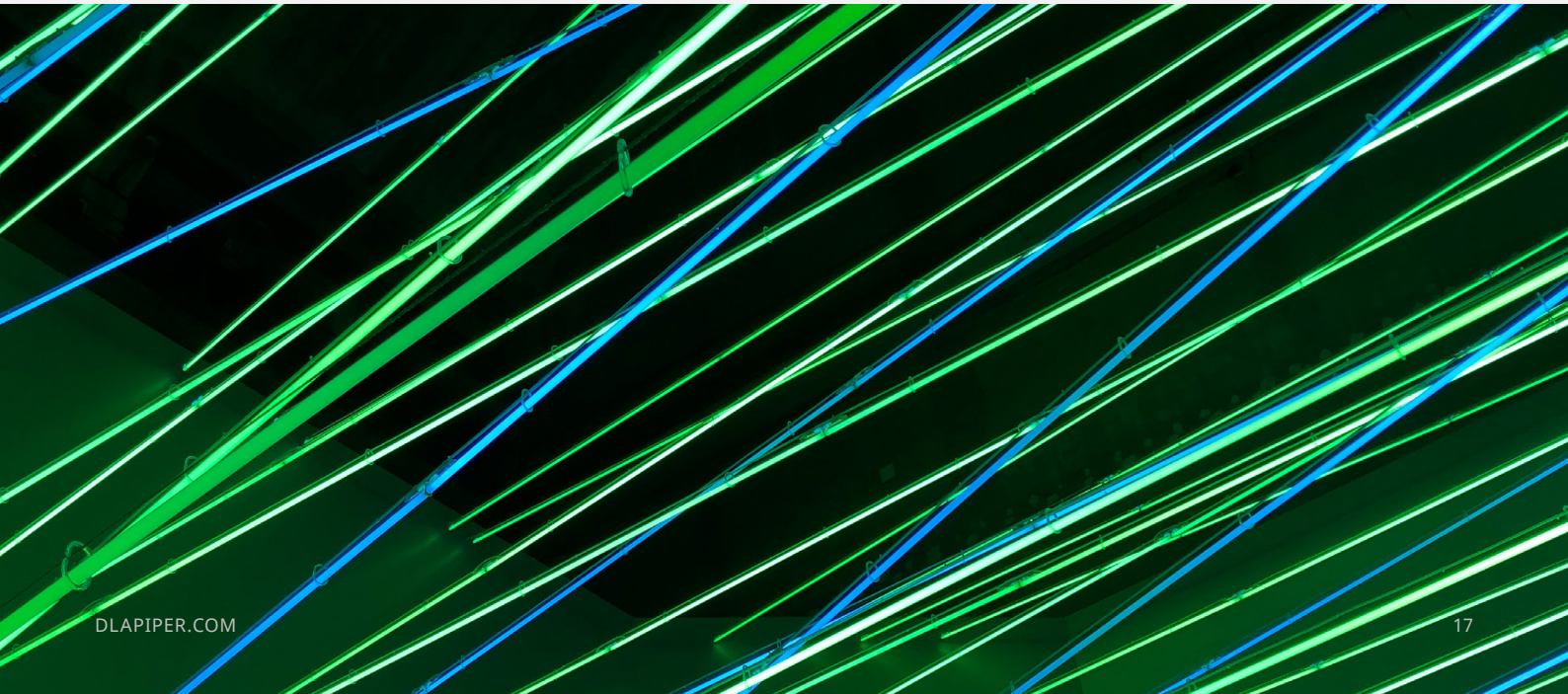
1. **Commercial solution customization**: Purchasing a foundational platform and tailoring it through targeted development
2. **Modular integration**: Combining purchased solutions for standardized functions with internally developed components for unique processes
3. **Vendor partnerships**: Collaborating with providers on co-development initiatives
4. **Progressive implementation**: Starting with purchased solutions for simpler use cases while building internal capabilities for more complex applications

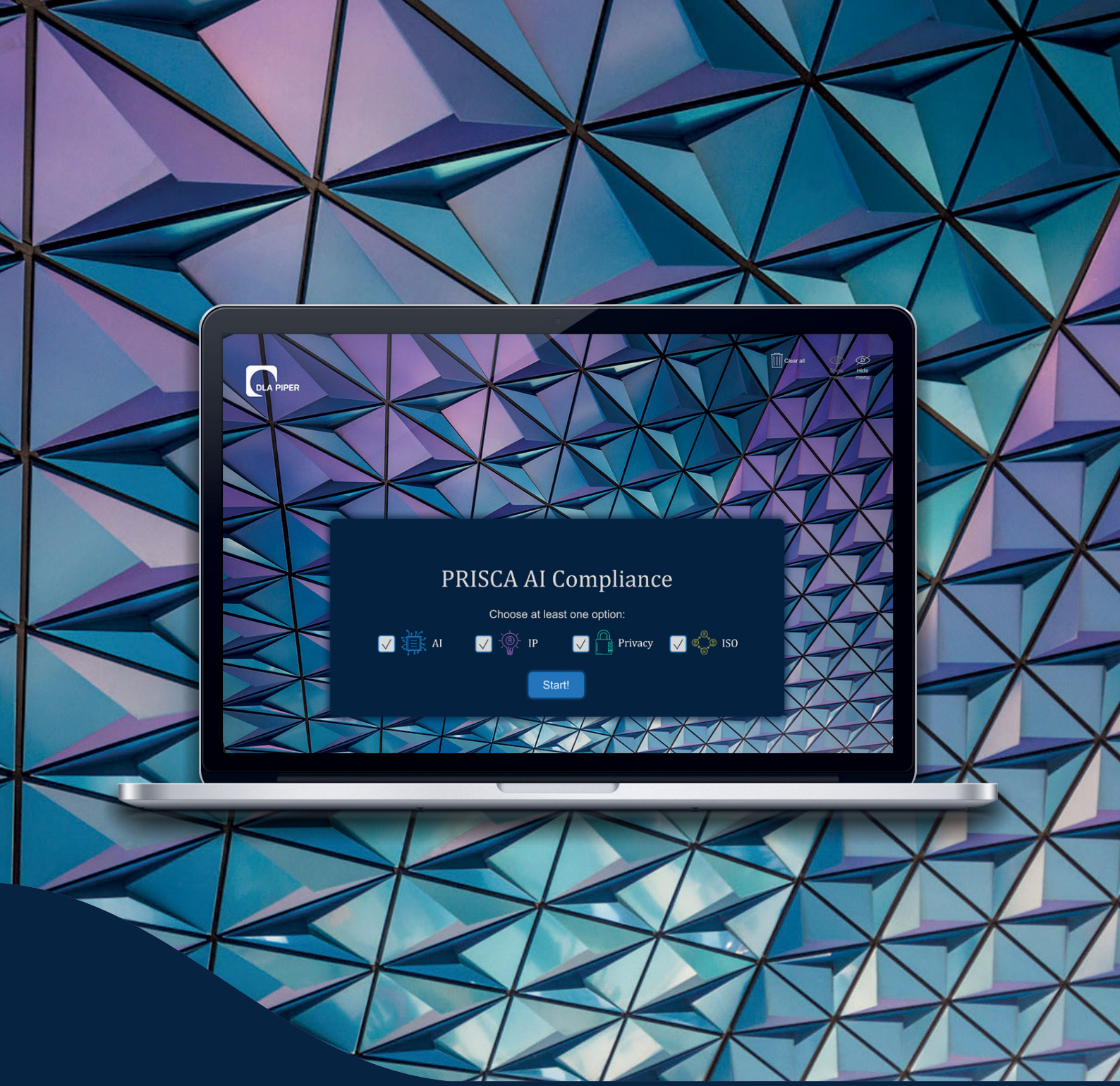
Conclusion

The build vs. buy decision for legal AI isn't binary. The most effective approach often combines purchased solutions for standardized functions with targeted internal development for unique requirements.

What matters isn't how you get the technology, but whether it solves real problems and delivers measurable results.

Our team helps legal departments navigate this landscape with frameworks and strategies designed to deliver practical results while maintaining legal excellence. Let's discuss how we can help your specific situation.



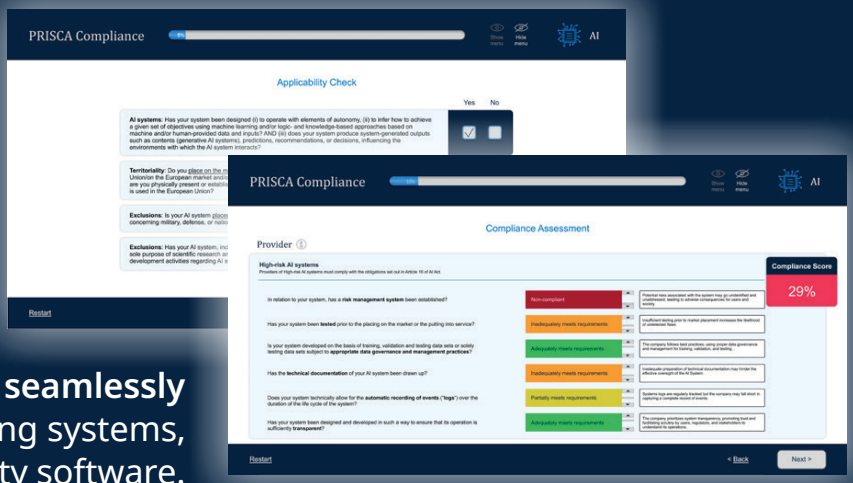


Prisca AI Compliance

Empowering Legal Compliance in the Age of Artificial Intelligence

Is your business ready to embrace the opportunities of AI, but worried about legal risks?

Introducing PRISCA AI Compliance by DLA Piper lawyers, a cutting-edge tool to assess your AI solutions' compliance with laws and ISO standards.



PRISCA AI Compliance **seamlessly integrates** into your existing systems, with no need for third-party software. It's available in **English** for global use.

Our unique weighted scoring algorithm generates a **compliance score** and an **easy-to-read report**. It highlights compliance with laws (privacy, IP, AI) and ISO standards.

Whether you're a user, provider, importer, or distributor of AI solutions, PRISCA AI Compliance supports your operations in **complying with regulations**.

Scan the QR Code to watch the video

Contact us for a demo:

giulio.coraggio@dlapiper.com
alessandro.ferrari@dlapiper.com
gualtiero.dragotti@dlapiper.com
elena.varese@dlapiper.com

Scan this qr code to access all issues of Diritto Intelligente

Contacts

Giulio Coraggio
Partner
Head of Intellectual Property and Technology, Italy
T +39 02 80 618 1
giulio.coraggio@dlapiper.com

Gualtiero Dragotti
Partner
Global Co-Chair, Patent Group
T +39 02 80 618 1
gualtiero.dragotti@dlapiper.com

Alessandro Ferrari
Partner
Head of Technology Sector, Italy
T +39 02 80 618 1
alessandro.ferrari@dlapiper.com

Roberto Valenti
Partner
Head of Life Sciences Sector, Italy
T +39 335 73 66 184
roberto.valenti@dlapiper.com

Elena Varese
Partner
Co-Head of Consumer Good, Food and Retail Sector, Italy
T +39 02 80 618 1
elena.varese@dlapiper.com

Ginevra Righini
Partner
T +39 02 80 61 863 4
ginevra.righini@dlapiper.com

Marco de Morpurgo
Partner
Global Co-Chair, Life Sciences
T +39 06 68 880 1
marco.demorpurgo@dlapiper.com

Alessandro Boso Caretta
Partner
T +39 06 68 880 1
alessandro.bosocaretta@dlapiper.com

dlapiper.com